Standar Nasional Indonesia

SNI 8848:2019

Manajemen risiko — Panduan implementasi SNI ISO 31000:2018 di sektor publik

ICS 03.100.01

Daftar isi

Prakata

Standar Nasional Indonesia (SNI) 8848:2019 dengan judul *Manajemen risiko — Panduan implementasi SNI ISO 31000:2018 di sektor publik*, merupakan SNI baru yang ditetapkan oleh Badan Standardisasi Nasional (BSN) Tahun 2019. Standar ini dimaksudkan untuk membantu organisasi sektor publik dalam menerapkan SNI ISO 31000:2018 di lingkungan oranisasinya, terutama dalam menerapkan prinsip-prinsip, kerangka kerja, dan proses manajemen risiko.

Standar ini disusun oleh Komite Teknis 03-10, *Tatakelola, Manajemen Risiko, dan Kepatuhan.* Standar ini telah dibahas dan disetujui dalam rapat konsensus nasional di Jakarta, pada tanggal 10 September 2019. Konsensus ini dihadiri oleh para pemangku kepentingan (*stakeholder*) terkait, yaitu perwakilan dari pelaku usaha, konsumen, pakar dan pemerintah.

Standar ini telah melalui tahap jajak pendapat pada tanggal 3 Oktober 2019 sampai dengan 2 Desember 2019 dengan hasil akhir disetujui menjadi SNI.

Dalam Standar ini terdapat klausul yang menggunakan acuan berdasarkan warna dan untuk menjamin kesamaan maksud dan pengertian, pengguna Standar ini disarankan menggunakan referensi Standar ini dalam bentuk dokumen cetakan (*print out*) dengan tinta berwarna.

Apabila pengguna menemukan keraguan dalam Standar ini, maka disarankan untuk melihat standar acuan normatif yang digunakan yaitu SNI ISO 31000:2018 *Manajemen Risiko – Pedoman.*

Perlu diperhatikan bahwa kemungkinan beberapa unsur dari dokumen Standar ini dapat berupa hak paten. BSN tidak bertanggung jawab untuk pengidentifikasian salah satu atau seluruh hak paten yang ada.

Pendahuluan

Keberadaan organisasi sektor publik tidak terlepas dari upaya suatu negara untuk terus meningkatkan kesejahteraan warga negaranya melalui berbagai pelayanan publik yang diberikan. Dalam memberikan pelayanan publik yang menjadi tugas dan tanggung jawabnya, organisasi sektor publik menghadapi berbagai ketidakpastian, baik yang berasal dari faktor eksternal maupun internal, yang kemudian melahirkan risiko dalam pencapaian sasaran organisasi.

Di Indonesia, definisi organisasi sektor publik dikenal dengan nama badan publik. Sesuai Undang-Undang nomor 14 tahun 2008, organisasi sektor publik adalah lembaga eksekutif, legislatif, yudikatif, dan sektor lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara (APBN) dan/atau Anggaran Pendapatan dan Belanja Daerah (APBD), atau organisasi non-pemerintah sepanjang sebagian atau seluruh dananya bersumber dari APBN dan/atau APBD, sumbangan masyarakat, dan/atau luar negeri.

Seiring dengan berkembangnya jumlah dan jenis risiko yang dihadapi oleh organisasi sektor publik, dibutuhkan penerapan manajemen risiko yang efektif dan terstandardisasi, serta sejalan dengan rujukan aturan dan peraturan yang relevan.

Standar ini disusun untuk melengkapi SNI ISO 31000:2018, *Manajemen risiko – Pedoman*, yang digunakan sebagai panduan bagi organisasi sektor publik dalam mengimplementasikan SNI ISO 31000:2018 yang terencana dan terstruktur, serta mampu melakukan penyesuaian dinamis pada saat terjadi perubahan dalam lingkungan internal dan eksternal organisasi sektor publik tersebut.

Standar ini diperlukan karena organisasi sektor publik memiliki karakteristik khusus sehingga memerlukan panduan pragmatis dalam menginternalisasi prinsip manajemen risiko, dalam membangun kerangka kerja manajemen risiko, dan dalam melaksanakan tahapan proses manajemen risiko. Standar ini dapat digunakan oleh orang dan/atau fungsi dalam organisasi sektor publik yang menciptakan dan melindungi nilai organisasinya untuk kepentingan publik melalui pengelolaan risiko.

Standar ini berisikan delapan bagian dengan penekanan pada bagian lima, enam, tujuh dan delapan yang merupakan inti dari Standar. Bagian lima mengenai peta jalan implementasi SNI ISO 31000:2018 di sektor publik, yang kemudian diikuti oleh bagian enam tentang panduan penerapan prinsip manajemen risiko, bagian tujuh tentang panduan penerapan kerangka kerja manajemen risiko, dan bagian delapan tentang panduan penerapan proses manajemen risiko di organisasi sektor publik.

Penyusunan standar ini juga dilatarbelakangi oleh amanat dari peraturan perundangan di Indonesia, yaitu:

- UUD 1945 Pasal 23 yang mengatur tentang Keuangan Negara; dan
- UU Nomor 17 Tahun 2003 tentang Keuangan Negara; dan
- UU Nomor 1 Tahun 2004 tentang Perbendaharaan Negara; serta
- PP Nomor 60 Tahun 2008 tentang Sistem Pengendalian Internal Pemerintah (SPIP).

Sistem Pengendalian Internal Pemerintah dibangun oleh 5 (lima) unsur yaitu: lingkungan pengendalian, penilaian risiko, kegiatan pengendalian, informasi dan komunikasi, serta pemantauan pengendalian intern. Untuk menerapkan unsur terkait penilaian risiko, organisasi sektor publik dapat menerapkan sistem manajemen risiko sesuai dengan Standar ini.

Manajemen risiko — Panduan implementasi SNI ISO 31000:2018 di sektor publik

1 Ruang lingkup

Standar ini menyediakan panduan untuk menerapkan SNI ISO 31000:2018 Manajemen Risiko – Pedoman, pada sektor publik yang diselenggarakan oleh organisasi sektor publik yaitu lembaga eksekutif, legislatif, yudikatif, dan lembaga negara atau sektor lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara (APBN) dan/atau Anggaran Pendapatan dan Belanja Daerah (APBD).

Standar ini tidak ditujukan untuk sektor publik yang diselenggarakan oleh organisasi sektor publik yang dananya bersumber dari kekayaan negara yang dipisahkan.

CATATAN 1 Contoh organisasi sektor publik yang dananya bersumber dari kekayaan negara yang dipisahkan adalah Badan Usaha Milik Negara (BUMN) dan Badan Usaha Milik Daerah (BUMD).

CATATAN 2 BUMN dan BUMD dapat menerapkan manajemen risiko dengan menggunakan langsung SNI ISO 31000:2018.

2 Acuan normatif

Dokumen berikut, secara keseluruhan atau sebagian, adalah acuan normatif dalam dokumen Standar ini dan mutlak diperlukan untuk penerapannya. Untuk acuan bertanggal, hanya menerapkan edisi yang dikutip. Untuk acuan tidak bertanggal, diterapkan edisi terbaru dari dokumen acuan tersebut - termasuk amandemennya:

– SNI ISO 31000:2018 *Manajemen Risiko – Pedoman*

3 Istilah dan definisi

Untuk keperluan Standar ini, selain istilah dan definisi yang terdapat di dalam SNI ISO 31000:2018, berlaku istilah dan definisi berikut:

3.1
manajemen puncak
orang atau kelompok orang yang mengarahkan dan mengendalikan organisasi di tingkat tertinggi

CATATAN Manajemen puncak pada organisasi sektor publik terdiri dari dua lingkup, yaitu:

a) Pimpinan Lembaga Negara, Menteri dan Kepala Daerah;

b) Pejabat pimpinan tinggi yang terdiri dari pejabat pimpinan utama, madya dan pratama.

3.2
pengawasan intern
aparat pada organisasi sektor publik yang melakukan seluruh proses kegiatan audit, reviu, evaluasi, pemantauan, dan kegiatan pengawasan lain terhadap penyelenggaraan tugas dan fungsi organisasi dalam rangka memberikan keyakinan yang memadai bahwa kegiatan telah dilaksanakan sesuai dengan tolok ukur yang telah ditetapkan secara efektif dan efisien untuk kepentingan pimpinan dalam mewujudkan tata kepemerintahan yang baik

CATATAN Orang atau fungsi yang melakukan pengawasan intern disebut pengawas internal.

3.3
model tiga lini pertahanan (*three lines of defense*)
model koordinasi manajemen risiko dalam suatu organisasi yang membagi fungsi organisasi menjadi tiga lini pertahanan terhadap risiko, yang terdiri atas pengelolaan risiko yang dilaksanakan oleh pemilik risiko, pengawasan risiko yang dilaksanakan oleh satuan kerja manajemen risiko, serta penyedia asurans independen yang dilaksanakan oleh pemeriksa

CATATAN Pada lini pertahanan kedua, fungsi pengawasan risiko dapat dilakukan oleh satuan kerja manajemen risiko bersama dengan satuan kerja lainnya yang bertugas mengawasi suatu jenis risiko tertentu seperti satuan kerja kepatuhan; satuan kerja keamanan, kesehatan dan keselamatan kerja; satuan kerja mutu; dan lainnya.

4 Manfaat pengimplementasian SNI ISO 31000:2018

Tujuan implementasi manajemen risiko di organisasi pada dasarnya adalah untuk menciptakan dan melindungi nilai organisasi dalam rangka mencapai visi misi yang telah ditetapkan. Pencapaian terhadap tujuan tersebut akan memberikan manfaat bagi organisasi sektor publik, sedikitnya mencakupi hal berikut:

- memberikan pelayanan publik;
- memastikan tercapainya tujuan utama;
- meningkatkan kesempatan dalam memanfaatkan peluang;
- meningkatkan kualitas perencanaan dan pencapaian kinerja;
- meningkatkan hubungan baik dengan pemangku kepentingan;
- meningkatkan kualitas pengambilan keputusan;
- meningkatkan rasa aman bagi pimpinan dan seluruh pegawai;
- meningkatkan akuntabilitas dan tata kelola organisasi; dan
- mengurangi kejutan (*surprises*).

5 Peta jalan pengimplementasian SNI ISO 31000:2018

Peta jalan dibutuhkan pada saat awal perancangan implementasi manajemen risiko untuk membantu pimpinan dan manajemen puncak organisasi sektor publik dalam menjaga arah implementasi SNI ISO 31000:2018 dalam koridor pencapaian sasaran jangka panjang organisasi, termasuk tonggak-tonggak capaian (*milestones*), alokasi sumber daya, pantauan dan pemastian kemajuan tahapan implementasi.

Peta jalan terdiri dari daftar aktivitas yang harus dilakukan oleh organisasi untuk memperoleh keluaran yang membawa hasil sebagai berikut:

- pembangunan infrastruktur, agar terjadi kesiapan penerapan manajemen risiko di seluruh organisasi;
- pembangunan kapasitas, agar penerapan manajemen risiko dapat memberikan manfaat dan bukan sekedar kepatuhan;
- pengintegrasian manajemen risiko, agar manajemen risiko menjadi bagian terpadu dari keseluruhan proses dalam organisasi; dan

– pembangunan budaya sadar risiko, agar tumbuh kesadaran tanggung jawab manajemen risiko pada setiap orang dalam organisasi.

CATATAN Contoh peta jalan pengimplementasian manajemen risiko tersedia di lampiran A.

6 Penerapan prinsip manajemen risiko

6.1 Umum

Penerapan prinsip manajemen risiko sesuai dengan SNI ISO 31000:2018 Pasal 4, Prinsip, ditunjukkan pada Gambar 1. Prinsip tersebut merupakan pondasi dalam mengimplementasikan kerangka kerja dan proses manajemen risiko dalam organisasi sektor publik untuk mencapai tujuan utama manajemen risiko.

Tujuan manajemen risiko adalah untuk menciptakan dan melindungi nilai. Tujuan manajemen risiko meningkatkan kinerja, mendorong inovasi, dan mendukung pencapaian sasaran.

Gambar 1 – Prinsip manajemen risiko

Sasaran organisasi sektor publik ditetapkan terlebih dahulu sehingga dapat digunakan sebagai rujukan dalam penciptaan dan pelindungan nilai organisasi tersebut.

Contoh sasaran umum organisasi sektor publik:

– meningkatkan kualitas pelayanan publik yang disediakan oleh organisasi;

– meningkatkan keefektifan alokasi dan efisiensi penggunaan sumber daya organisasi;

– meningkatkan kepatuhan terhadap kebijakan formal (Undang-Undang, Hukum dan Regulasi);

– meningkatkan kepercayaan pemangku kepentingan;

– meningkatkan ketahanan organisasi; dan

– meningkatkan keandalan laporan pertanggungjawaban organisasi.

6.2 Prinsip terintegrasi

6.2.1 Prinsip

Sesuai SNI ISO 31000:2018 Pasal 4, prinsip terintegrasi (prinsip a), manajemen risiko adalah bagian integral dari semua aktivitas organisasi.

6.2.2 Bagaimana menerapkan prinsip terintegrasi pada organisasi sektor publik

Agar manajemen risiko menjadi bagian integral dari semua aktivitas organisasi, manajemen puncak organisasi sektor publik memastikan sedikitnya hal di bawah ini:

- kerangka kerja dan program manajemen risiko berkontribusi terhadap proses perencanaan strategi, penetapan anggaran, pelaksanaan strategi, dan pelaporan organisasi; dan
- adanya kebijakan formal sebagai dasar instruksi yang menggambarkan serta mendokumentasikan tautan antara sistem manajemen risiko dengan sistem manajemen lainnya.

6.3 Prinsip terstruktur dan komprehensif

6.3.1 Prinsip

Sesuai SNI ISO 31000:2018 Pasal 4, prinsip terstruktur dan komprehensif (prinsip b), pendekatan terstruktur dan komprehensif terhadap manajemen risiko berkontribusi terhadap hasil yang konsisten dan terstruktur.

6.3.2 Bagaimana menerapkan prinsip terstruktur dan komprehensif pada organisasi sektor publik

Agar manajemen risiko berkontribusi terhadap hasil yang konsisten dan terstruktur, manajemen puncak organisasi sektor publik memastikan sedikitnya hal di bawah ini:

- penentuan sasaran telah memenuhi kriteria SMART-C yaitu *Specific* (spesifik), *Measurable* (terukur), *Attainable* (dapat dicapai), *Relevant* (relevan), *Time Bound* (batas waktu) dan *Challenging* (menantang); dan
- proses bisnis dalam mencapai sasaran dapat terpetakan dan tertelusuri secara sistematis.

6.4 Prinsip disesuaikan

6.4.1 Prinsip

Sesuai SNI ISO 31000:2018 Pasal 4, prinsip disesuaikan (prinsip c), kerangka kerja dan proses manajemen risiko disesuaikan dan proporsional dengan konteks eksternal dan internal organisasi yang berkaitan dengan sasarannya.

6.4.2 Bagaimana menerapkan prinsip disesuaikan pada organisasi sektor publik

Agar manajemen risiko sesuai dan proporsional dengan konteks, manajemen puncak organisasi sektor publik memastikan sedikitnya hal di bawah ini:

- adanya proses formal penentuan konteks internal dan eksternal organisasi termasuk pemetaan keterlibatan dan/atau pengaruh pemangku kepentingan; dan

- kerangka kerja dan proses manajemen risiko dijalankan seiring dengan kebijakan formal yang relevan dan berlaku bagi organisasi, misal: Undang-Undang, Hukum dan Regulasi.

6.5 Prinsip inklusif

6.5.1 Prinsip

Sesuai SNI ISO 31000:2018 Pasal 4, prinsip inklusif (prinsip d), pelibatan yang sesuai dan tepat waktu dari pemangku kepentingan memungkinkan pengetahuan, pandangan, dan persepsi mereka untuk dipertimbangkan. Hal ini menghasilkan peningkatan kesadaran dan manajemen risiko terinformasi.

6.5.2 Bagaimana menerapkan prinsip inklusif pada sektor publik

Agar manajemen risiko inklusif, manajemen puncak organisasi sektor publik memastikan sedikitnya hal di bawah ini:

- memiliki program pemangku kepentingan dalam rangka pengkinian informasi mengenai kebutuhan dan/atau harapan pemangku kepentingan terhadap pelayanan publik organisasi; dan
- masukan dari pemangku kepentingan dipertimbangkan oleh organisasi dalam kerangka manajemen risiko terutama tahap rancangan, implementasi dan evaluasi.

6.6 Prinsip dinamis

6.6.1 Prinsip

Sesuai SNI ISO 31000:2018 Pasal 4, prinsip dinamis (prinsip e), risiko dapat muncul, berubah, atau hilang seiring perubahan konteks eksternal dan internal organisasi. Manajemen risiko mengantisipasi, mendeteksi, mengakui, dan menanggapi perubahan dan peristiwa tersebut secara sesuai dan tepat waktu.

6.6.2 Bagaimana menerapkan prinsip dinamis pada organisasi sektor publik

Agar manajemen risiko dinamis seiring perubahan konteks, manajemen puncak organisasi sektor publik memastikan sedikitnya hal di bawah ini:

- kajian terhadap efektivitas kerangka dan proses manajemen risiko sebaiknya dilakukan secara berkala dan/atau bila ada perubahan konteks organisasi baik eksternal maupun internal; dan
- memasukkan pandangan baik jangka pendek maupun jangka panjang dalam penentuan konteks sehingga dinamika risiko (baik baru maupun lama) dapat ditemukenali seawal mungkin.

6.7 Prinsip informasi terbaik yang tersedia

6.7.1 Prinsip

Sesuai SNI ISO 31000:2018 Pasal 4, prinsip informasi terbaik yang tersedia (prinsip f), masukan manajemen risiko didasarkan atas informasi historis dan saat ini, dan juga harapan masa depan. Manajemen risiko secara eksplisit memperhitungkan segala batasan dan ketidakpastian yang berkaitan dengan informasi dan harapan tersebut. Informasi sebaiknya tepat waktu, jelas, dan tersedia bagi pemangku kepentingan yang relevan.

6.7.2 Bagaimana menerapkan prinsip informasi terbaik yang tersedia pada organisasi sektor publik

Agar manajemen risiko terdukung oleh informasi terbaik yang tersedia, manajemen puncak organisasi sektor publik memastikan sedikitnya hal di bawah ini:

- pengkinian berkala terhadap pangkalan data dan informasi yang relevan bagi organisasi untuk kegunaan pengembangan kebijakan publik dan implementasinya; dan
- kecukupan dan kualitas informasi ditingkatkan dari waktu ke waktu sehingga pengambilan keputusan dapat dilakukan oleh manajemen puncak organisasi secara tepat waktu, dan tepat sasaran.

6.8 Prinsip faktor manusia dan budaya

6.8.1 Prinsip

Sesuai SNI ISO 31000:2018 Pasal 4, prinsip faktor manusia dan budaya (prinsip g), perilaku dan budaya manusia secara signifikan memengaruhi semua aspek manajemen risiko pada semua tingkat dan tahap.

6.8.2 Bagaimana menerapkan prinsip faktor manusia dan budaya pada organisasi sektor publik

Agar manajemen risiko selalu memperhitungkan faktor manusia dan budaya, manajemen puncak organisasi sektor publik memastikan sedikitnya hal di bawah ini:

- adanya peta pembangunan (*development*), penyebaran (*deployment*) dan pematangan budaya sadar risiko organisasi; dan
- pembangunan infrastruktur sumber daya manusia baik jumlah maupun kompetensi yang memadai untuk penerapan manajemen risiko organisasi.

6.9 Prinsip perbaikan berkelanjutan

6.9.1 Prinsip

Sesuai SNI ISO 31000:2018 Pasal 4, prinsip perbaikan berkelanjutan (prinsip h), manajemen risiko diperbaiki secara berkelanjutan melalui pelajaran dan pengalaman.

6.9.2 Bagaimana menerapkan prinsip tersebut pada organisasi sektor publik

Agar manajemen risiko dapat ditingkatkan keefektifannya secara berkelanjutan, manajemen puncak organisasi sektor publik memastikan sedikitnya hal di bawah ini:

- keefektifan manajemen risiko diukur secara berkala dan selalu ditingkatkan dari waktu ke waktu; dan
- adanya peta jalan untuk pengembangan tingkat maturitas (*maturity level*) dari penerapan manajemen risiko.

7 Penerapan kerangka kerja manajemen risiko

7.1 Umum

Penerapan kerangka kerja manajemen risiko sesuai dengan SNI ISO 31000:2018 Pasal 5, ditunjukkan pada Gambar 2. Kerangka kerja tersebut memberikan panduan bagi organisasi sektor publik untuk mengintegrasikan manajemen risiko ke dalam aktivitas dan fungsi yang signifikan. Keefektifan manajemen risiko bergantung pada integrasinya ke dalam tata kelola organisasi, termasuk pengambilan keputusan.

Tujuan kerangka kerja manajemen risiko adalah untuk membantu organisasi dalam mengintegrasikan manajemen risiko ke dalam aktivitas dan fungsi signifikan. Efektivitas manajemen risiko bergantung pada integrasinya ke dalam tata kelola organisasi, termasuk pengambilan keputusan. Ini memerlukan dukungan dari pemangku kepentingan, khususnya manajemen puncak.

Gambar 2 – Kerangka kerja manajemen risiko

7.2 Kerangka kerja kepemimpinan dan komitmen

7.2.1 Kerangka kerja

Sesuai SNI ISO 31000:2018 Pasal 5.2, manajemen puncak dan badan pengawas, jika memungkinkan, sebaiknya memastikan manajemen risiko terintegrasi pada semua aktivitas organisasi dan sebaiknya menunjukkan kepemimpinan dan komitmen dengan:

- menyesuaikan dan mengimplementasikan semua komponen kerangka kerja;
- menerbitkan pernyataan atau kebijakan yang menetapkan pendekatan, rencana, atau arah tindakan manajemen risiko;
- memastikan sumber daya yang diperlukan dialokasikan untuk pengelolaan risiko; dan
- menetapkan kewenangan, tanggung jawab, dan akuntabilitas pada tingkat yang diperlukan di dalam organisasi.

Manajemen puncak memiliki akuntabilitas untuk mengelola risiko, sedangkan badan pengawas memiliki akuntabilitas untuk mengawasi pelaksanaan manajemen risiko. Badan pengawas sering diharapkan atau diperlukan untuk:

- memastikan risiko dipertimbangkan dengan memadai saat penetapan sasaran organisasi;
- memahami risiko yang dihadapi organisasi dalam mencapai sasarannya;
- memastikan sistem untuk mengelola risiko tersebut diterapkan dan dijalankan dengan efektif;
- memastikan sistem tersebut sesuai dengan konteks sasaran organisasi; dan
- memastikan tersedianya informasi yang cukup tentang risiko yang dihadapi dan dikelola oleh organisasi serta memastikan pengkomunikasiannya dengan tepat.

7.2.2 Bagaimana menerapkan komponen kerangka kerja kepemimpinan dan komitmen pada organisasi sektor publik

Penerapan komponen kerangka kerja kepemimpinan dan komitmen pada organisasi sektor publik dilakukan dengan:

- menyamakan persepsi dan pemahaman pemimpin dan manajemen puncak mengenai SNI ISO 31000:2018, serta memastikan pemimpin dan manajemen puncak memiliki kompetensi manajemen risiko yang memadai terkait dengan fungsi dan peran mereka;
- melaksanakan program manajemen risiko agar menjadi akuntabilitas pemimpin dan manajemen puncak, dan secara eksplisit tertera dalam kontrak manajemen (atau yang sederajat) antara mereka dengan pemegang kepentingan;
- membentuk unit manajemen risiko dalam struktur lembaga organisasi yang mendukung pemimpin dan manajemen puncak dalam mengembangkan rencana sampai dengan implementasi manajemen risiko secara keseluruhan; dan
- membangun kapasitas dan kapabilitas manajemen risiko di seluruh tingkatan organisasi baik terkait dengan infrastruktur keras misal komputerisasi maupun lunak dan/atau kompetensi sumber daya manusia.

CATATAN 1 Perwujudan kepemimpinan dan komitmen sedikitnya ditunjukkan dengan ketersediaan:

- kebijakan dan pedoman formal manajemen risko yang menjadi pondasi penyesuaian proses bisnis berbasis risiko. Dalam pedoman tersebut sebaiknya terdapat pernyataan selera risiko dan toleransi risiko tingkat organisasi;
- program manajemen risiko menjadi bagian dari strategi atau rencana jangka panjang, serta dipantau dan dievaluasi secara berkala;
- struktur manajemen risiko dengan sumber daya manusia yang memadai sebagai perwujudan praktik tata kelola yang baik dan pemenuhan akuntabilitas pimpinan dan manajemen puncak;
- anggaran yang cukup dan memadai untuk mendukung program manajemen risiko baik dalam pembangunan kapasitas infrastruktur maupun dalam perjalananan implementasinya;
- ketersediaan dan akses informasi yang mencukupi dalam pengelolaan risiko sehingga informasi yang dibutuhkan untuk pengambilan keputusan dapat dijalankan tepat waktu dan tepat sasaran; dan
- adanya keterlibatan pemangku kepentingan dalam penentuan sasaran yang dijadikan acuan dalam proses manajemen risiko.

CATATAN 2 Kebijakan formal (Undang-Undang, Hukum dan Regulasi) merupakan pondasi implementasi manajemen risiko pada suatu organisasi sektor publik. Peraturan tersebut bertujuan untuk mengatur agar organisasi dapat mencapai tujuan yang telah ditetapkan.

CATATAN 3 Bentuk produk hukum dari regulasi internal atau payung hukum sesuai dengan kebutuhan masing-masing organisasi sektor publik, misal:

- kementerian dalam bentuk: peraturan menteri (Permen) dan keputusan menteri (Kepmen);
- lembaga pemerintah non kementerian dalam bentuk: peraturan Lembaga Pemerintah Non Kementerian (LPNK); dan
- pemerintah daerah dalam bentuk: peraturan daerah dan peraturan kepala daerah tingkat provinsi, kabupaten, dan kota.

7.3 Kerangka kerja integrasi

7.3.1 Kerangka kerja

Sesuai SNI ISO 31000:2018 Pasal 5.3, integrasi manajemen risiko bergantung pada pemahaman terhadap struktur dan konteks organisasi. Struktur berbeda bergantung pada tujuan, sasaran, dan kompleksitas organisasi. Risiko dikelola di semua bagian struktur organisasi. Tiap orang di organisasi bertanggung jawab terhadap pengelolaan risiko.

Tata kelola memandu arah organisasi, hubungan eksternal dan internalnya, serta peran, proses, dan praktik yang diperlukan untuk mencapai tujuannya. Struktur manajemen menerjemahkan arahan tata kelola menjadi strategi dan sasaran terkait yang diperlukan untuk mencapai tingkat yang diinginkan dari kinerja berkelanjutan dan viabilitas jangka panjang. Penentuan akuntabilitas dan peran pengawasan manajemen risiko di dalam organisasi adalah bagian integral dari tata kelola organisasi.

Integrasi manajemen risiko ke dalam organisasi adalah proses yang dinamis dan berulang, serta sebaiknya disesuaikan dengan kebutuhan dan budaya organisasi. Manajemen risiko sebaiknya menjadi bagian dari, dan tidak terpisahkan dari, tujuan, tata kelola, kepemimpinan dan komitmen, strategi, sasaran, dan operasi organisasi.

7.3.2 Bagaimana menerapkan komponen kerangka kerja integrasi pada organisasi sektor publik

Penerapan komponen kerangka kerja integrasi tersebut pada organisasi sektor publik dilakukan dengan:

- memetakan konteks eksternal dan internal secara metodis dan terukur sehingga organisasi dapat membuat kategori dan kriteria risiko yang sudah mempertimbangkan harapan dan tuntutan mereka;
- menerapkan manajemen risiko sebagai bagian terpadu dari praktik tata kelola organisasi, sehingga prinsip-prinsip tata kelola tertanam dalam penerapan manajemen risiko;
- menerapkan manajemen risiko untuk mencapai sasaran jangka panjang dan jangka pendek organisasi sehingga terkait dengan keberlanjutan organisasi dalam penciptaan dan perlindungan nilai, mulai dari penetapan sasaran, formulasi strategi dan implementasinya, serta pengembangan proses bisnis untuk mencapai sasaran, sampai pada pelaporan akuntabilitas organisasi; dan
- membuat peta jalan penerapan manajemen risiko yang secara eksplisit menggambarkan tahapan integrasi sistem manajemen risiko dengan sistem manajemen lainnya dalam organisasi.

CATATAN Pengintegrasian manajemen risiko ke dalam proses organisasi dapat dilakukan secara bertahap atau langsung bersamaan.

7.4 Kerangka kerja desain

7.4.1 Kerangka kerja

Sesuai SNI ISO 31000:2018 Pasal 5.4.1, ketika mendesain kerangka kerja pengelolaan risiko, organisasi sebaiknya memeriksa dan memahami konteks eksternal dan internalnya.

Pemeriksaan konteks eksternal organisasi dapat termasuk, tetapi tidak terbatas kepada:

- faktor sosial, budaya, politik, hukum, regulasi, keuangan, teknologi, ekonomi, dan lingkungan, baik internasional, nasional, regional, maupun lokal;
- penggerak dan tren utama yang memengaruhi sasaran organisasi;
- hubungan, persepsi, nilai, kebutuhan, dan harapan pemangku kepentingan eksternal;
- hubungan dan komitmen kontraktual; dan
- kompleksitas dan dependensi jaringan.

Pemeriksaan konteks internal organisasi dapat termasuk, tetapi tidak terbatas kepada:

- visi, misi, dan nilai;
- tata kelola, struktur organisasi, peran, dan akuntabilitas;
- strategi, sasaran, dan kebijakan;
- budaya organisasi;
- standar, panduan, dan model yang diadopsi oleh organisasi;
- kapabilitas, ditinjau dari sumber daya dan pengetahuan (misalnya modal, waktu, orang, kekayaan intelektual, proses, sistem, dan teknologi);
- data, sistem informasi, dan alir informasi;
- hubungan dengan pemangku kepentingan internal, dengan mempertimbangkan persepsi dan nilai mereka;
- hubungan dan komitmen kontraktual; dan
- interdependensi dan interkoneksi.

Sesuai SNI ISO 31000:2018 Pasal 5.4.2, manajemen puncak dan badan pengawas, jika memungkinkan, sebaiknya menunjukkan dan menegaskan komitmen berkelanjutan mereka terhadap manajemen risiko melalui kebijakan, pernyataan, atau bentuk lain yang secara jelas menyampaikan sasaran dan komitmen organisasi terhadap manajemen risiko. Komitmen sebaiknya termasuk, tetapi tidak terbatas kepada:

- tujuan pengelolaan risiko organisasi serta kaitan dengan sasaran dan kebijakan lain;
- penguatan kebutuhan untuk mengintegrasikan manajemen risiko ke dalam keseluruhan budaya organisasi;
- kepemimpinan dalam integrasi manajemen risiko ke dalam aktivitas bisnis inti dan pengambilan keputusan;
- kewenangan, tanggung jawab, dan akuntabilitas;
- penyediaan sumber daya yang diperlukan;

- cara penanganan konflik kepentingan;
- pengukuran dan pelaporan dalam indikator kinerja organisasi; dan
- tinjauan dan peningkatan.

Komitmen manajemen risiko sebaiknya dikomunikasikan di dalam organisasi dan kepada pemangku kepentingannya.

Sesuai SNI ISO 31000:2018 Pasal 5.4.3, manajemen puncak dan badan pengawas, sesuai penerapan, sebaiknya memastikan bahwa kewenangan, tanggung jawab, dan akuntabilitas untuk peran yang relevan dalam manajemen risiko telah ditetapkan dan dikomunikasikan pada semua tingkat organisasi, serta sebaiknya:

- menekankan bahwa manajemen risiko adalah tanggung jawab inti; dan
- mengidentifikasi individu yang memiliki akuntabilitas dan kewenangan untuk mengelola risiko (pemilik risiko).

Sesuai SNI ISO 31000:2018 Pasal 5.4.4, manajemen puncak dan badan pengawas, sesuai penerapan, sebaiknya memastikan alokasi sumber daya manajemen risiko yang memadai, yang dapat termasuk, tetapi tidak terbatas pada:

- orang, keterampilan, pengalaman, dan kompetensi;
- proses, metode, dan alat yang dipakai organisasi untuk mengelola risiko;
- proses dan prosedur terdokumentasi;
- sistem manajemen informasi dan pengetahuan; dan
- pengembangan profesional dan kebutuhan pelatihan;

Organisasi sebaiknya mempertimbangkan kapabilitas, dan keterbatasan, sumber daya yang ada.

Sesuai SNI ISO 31000:2018 Pasal 5.4.5, organisasi sebaiknya menetapkan pendekatan yang disetujui untuk komunikasi dan konsultasi guna mendukung kerangka kerja dan memfasilitasi penerapan efektif manajemen risiko. Komunikasi melibatkan pembagian informasi dengan audiens yang dituju. Konsultasi juga melibatkan pemberian umpan balik dari partisipan dengan harapan bahwa hal itu dapat berkontribusi dan membentuk keputusan atau aktivitas lain.

Metode dan konten komunikasi dan konsultasi sebaiknya mencerminkan harapan pemangku kepentingan, jika relevan.

Komunikasi dan konsultasi sebaiknya tepat waktu dan memastikan bahwa informasi yang relevan dikumpulkan, digabungkan, disintesis, dan dibagikan, secara sesuai, serta bahwa umpan balik diberikan dan peningkatan dibuat.

7.4.2 Bagaimana menerapkan komponen kerangka kerja desain pada organisasi sektor publik

Penerapan komponen kerangka kerja desain pada organisasi sektor publik dilakukan dengan:

- membuat pemetaan konteks eksternal dan internal dilakukan secara metodis dan terukur sehingga organisasi dapat membuat desain manajemen risiko yang sudah mempertimbangkan kategori dan kriteria risiko sejalan dengan harapan dan tuntutan pemangku kepentingan;
- membuat kontrak manajemen antara pimpinan dan manajemen puncak dengan para pegawai terutama pemberi mandat, yang secara eksplisit menyatakan bahwa penerapan manajemen risiko adalah akuntabilitas pimpinan dan manajemen puncak yang menjadi ukuran kinerja mereka;
- menjelaskan struktur manajemen risiko yang berbentuk model tiga lini pertahanan yang memberikan kejelasan tata kelola risiko (*risk governance*) yang meliputi sedikitnya: tugas dan tanggung jawab pimpinan dan manajemen puncak dalam penerapan manajemen risiko; dan
- membuat kebijakan di tingkat lembaga sebagai acuan strategi dan peta jalan penerapan manajemen risiko mulai dari pembangunan kapasitas dan kapabilitas sampai dengan proses pelaporan akuntabilitas pimpinan dan manajemen puncak, serta pembangunan, penyebaran dan pematangan budaya sadar risiko;
- menyusun program pengembangan kapasitas manajemen risiko organisasi yang mencakupi penetapan jumlah, kualifikasi kompetensi, terdiri atas pengetahuan, keterampilan, dan sikap dalam menerapkan manajemen risiko berbasis SNI ISO 31000:2018, serta pengalaman sumber daya manusia yang dilibatkan dalam penerapan manajemen risiko, berikut dengan waktu pelaksanaan yang diselaraskan dengan peta jalan pengimplementasian manajemen risiko yang dimiliki organisasi;
- mengalokasikan anggaran yang dibutuhkan untuk mendukung pelaksanaan program pembangunan dan pengembangan kapasitas manajemen risiko organisasi, termasuk pengembangan sistem informasi manajemen risiko, pengintegrasian sistem manajemen risiko dengan sistem manajemen lainnya sampai pada tingkat proses bisnis, dan pembangunan, penyebaran serta pematangan budaya sadar risiko; dan
- membuat panduan strategi komunikasi dan konsultasi, serta rambu-rambu pelaksanaannya agar organisasi memperoleh informasi memadai tentang tuntutan dan harapan pemangku kepentingan, sehingga program pelibatan dan sosialisasi manajemen risiko menjadi efektif dan efisien baik dalam pengembangan materi atau substansi dan media penyampaiannya.

CATATAN 1 Organisasi dapat menggunakan berbagai metode komunikasi dan konsultasi. Salah satu metode yang sering digunakan adalah matriks RACI untuk mendeteksi tingkat keterlibatan para pihak dalam suatu kegiatan penanganan risiko. RACI adalah singkatan dari *Responsible, Accountable, Consulted,* dan *Informed*.

CATATAN 2 Contoh pembentukan struktur manajemen risiko tersedia di lampiran B.

CATATAN 3 Contoh kebijakan manajemen risiko tersedia di lampiran C.

CATATAN 4 Contoh pengembangan budaya sadar risiko tersedia di lampiran D.

7.5 Kerangka kerja implementasi

7.5.1 Kerangka kerja

Sesuai SNI ISO 31000:2018 Pasal 5.5, organisasi sebaiknya mengimplementasikan kerangka kerja manajemen risiko dengan:

- mengembangkan rencana yang sesuai, termasuk waktu dan sumber daya;
- mengidentifikasi di mana, kapan, bagaimana, dan oleh siapa beragam jenis keputusan dibuat di seluruh organisasi;
- memodifikasi proses pengambilan keputusan yang sesuai; jika diperlukan; dan
- memastikan pengaturan organisasi dalam mengelola risiko dipahami dengan jelas dan dipraktikkan.

Implementasi kerangka kerja yang berhasil memerlukan keterlibatan dan kesadaran pemangku kepentingan.

7.5.2 Bagaimana menerapkan komponen kerangka kerja implementasi pada organisasi sektor publik

Penerapan komponen kerangka kerja implementasi pada organisasi sektor publik dilakukan dengan:

- memastikan manajemen puncak sebagai pemimpin risiko memiliki akuntabilitas dan tanggung jawab dalam menentukan arah dan sasaran penerapan manajemen risiko, mulai dari pengelolaan risiko strategis, operasional, dan kepatuhan secara terpadu;
- mensosialisasikan peta jalan implementasi manajemen risiko secara efektif kepada seluruh tingkatan organisasi, terukur, dipantau serta ditinjau ulang;
- memantau dan mengkaji efektivitas implementasi manajemen risiko dipantau dan dikaji ulang secara berkala agar organisasi mampu melakukan adaptasi yang diperlukan dalam rangka meningkatkan probabilitas capaian tujuan dan sasaran mereka; dan
- memastikan model tiga lini pertahanan sesuai dengan kebutuhan.

CATATAN Agar implementasi manajemen risiko dalam organisasi dapat berjalan efektif, manajemen puncak melakukan:

- pengembangan budaya sadar risiko;
- pembentukan struktur manajemen risiko; dan
- penyelenggaraan proses manajemen risiko secara menyeluruh.

7.6 Kerangka kerja evaluasi

7.6.1 Kerangka kerja

Sesuai SNI ISO 31000:2018 Pasal 5.6, untuk mengevaluasi efektivitas kerangka kerja manajemen risiko, organisasi sebaiknya:

- mengukur kinerja kerangka kerja manajemen risiko secara berkala terhadap tujuan, rencana implementasi, indikator, dan perilaku yang diharapkan; dan
- menentukan apakah kerangka kerja manajemen risiko tetap sesuai untuk mendukung pencapaian sasaran organisasi.

7.6.2 Bagaimana menerapkan komponen kerangka kerja evaluasi pada organisasi sektor publik

Penerapan komponen kerangka kerja evaluasi pada organisasi sektor publik dilakukan dengan:

- mengevaluasi efektivitas penerapan manajemen risiko dilakukan secara berkala dan teratur baik oleh penyedia jasa asurans internal maupun pihak independen eksternal;
- mengevaluasi penerapan standar secara keseluruhan maupun terhadap masing-masing komponen pendukungnya; dan
- menyampaikan hasil evaluasi untuk menjadi bahan tinjau ulang pimpinan dan manajemen puncak agar penerapan manajemen risiko tetap efektif, relevan dan kontekstual dengan perkembangan situasi, tantangan dan sasaran organisasi.

7.7 Kerangka kerja perbaikan

7.7.1 Kerangka kerja

Sesuai SNI ISO 31000:2018 Pasal 5.7.1, organisasi sebaiknya secara berkelanjutan memantau dan mengadaptasi kerangka kerja manajemen risiko untuk mengatasi perubahan eksternal dan internal. Dengan demikian, organisasi dapat meningkatkan nilainya.

Sesuai SNI ISO 31000:2018 Pasal 5.7.2, organisasi sebaiknya secara sinambung meningkatkan kesesuaian, kecukupan, dan efektivitas kerangka kerja manajemen risiko, serta bagaimana proses manajemen risiko diintegrasikan.

7.7.2 Bagaimana menerapkan komponen kerangka kerja perbaikan pada organisasi sektor publik

Penerapan komponen kerangka kerja tersebut pada organisasi sektor publik dilakukan dengan:

- memastikan pimpinan dan manajemen puncak menggunakan hasil evaluasi untuk meningkatkan kualitas dan efektivitas penerapan manajemen risiko; dan
- memastikan pimpinan dan manajemen puncak memiliki program pengembangan tingkat maturitas penerapan manajemen risiko (*risk management maturity*) yang terukur dan tervalidasi oleh pihak asurans internal dan atau pihak asurans independen eksternal.

CATATAN 1 Di bawah ini adalah model tingkat maturitas risiko yang dapat dipakai:

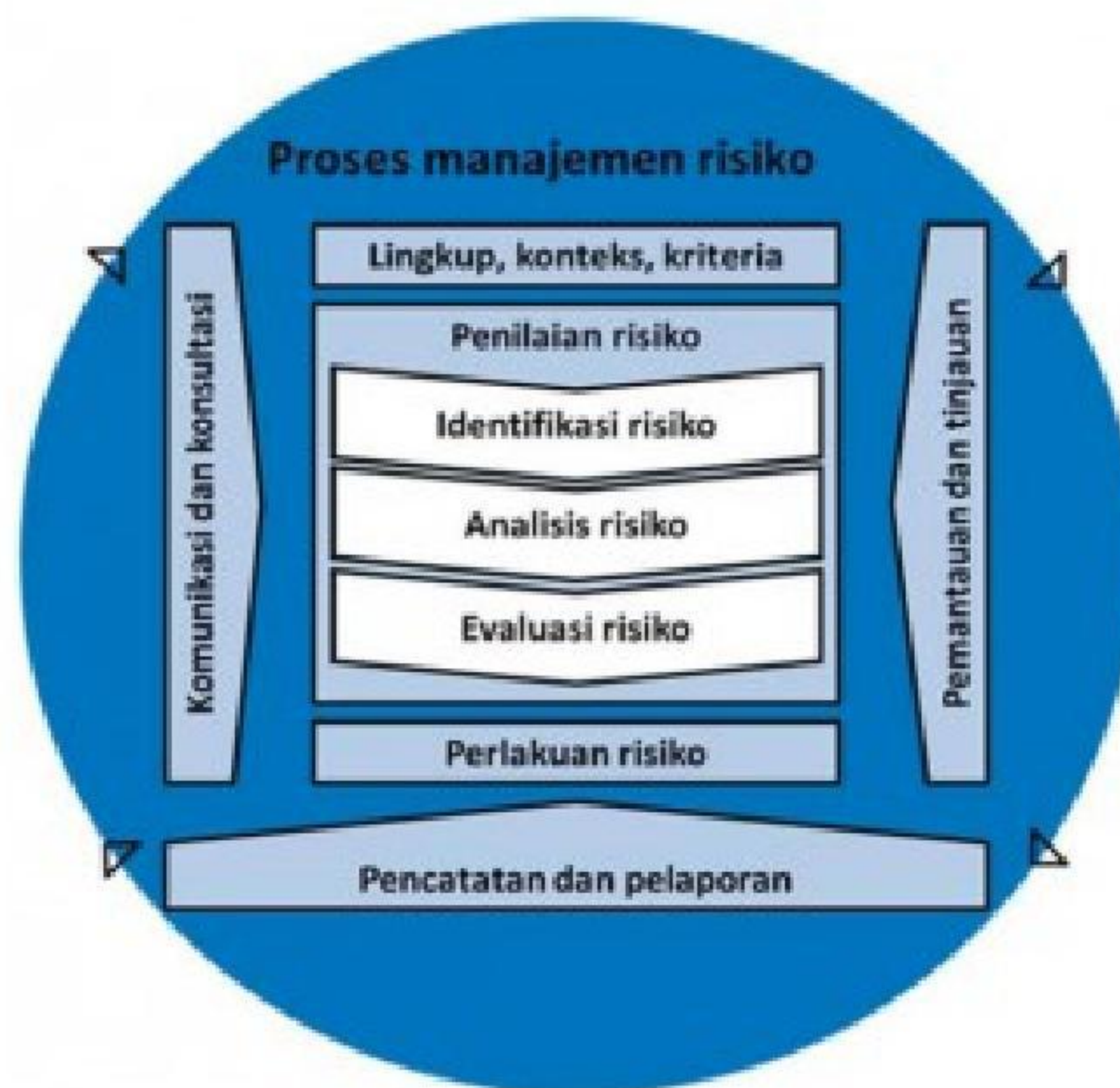
- tingkat maturitas 1: Belum sadar risiko (*risk naive*);
- tingkat maturitas 2: Sudah mulai sadar risiko (*risk aware*);
- tingkat maturitas 3: Sadar risiko dan risiko terdefinisi (*risk defined*);
- tingkat maturitas 4: Budaya sadar risiko tercipta dan risiko terkelola (*risk managed*); dan
- tingkat maturitas 5: Budaya sadar risiko optimal dan manajemen risiko sudah menjadi alat pemampu unggulan organisasi dalam pencapaian sasaran (*risk optimized*).

Tingkat maturitas semakin tinggi, semakin baik dan efektif.

CATATAN 2 Contoh model tingkat maturitas risiko tersedia di lampiran E.

8 Penerapan proses manajemen risiko

8.1 Umum

Proses manajemen risiko mencakupi langkah-langkah yang dijalankan secara sistematis berurutan dan iteratif mulai dari: Komunikasi dan konsultasi; Penetapan ruang lingkup, konteks, dan kriteria; Penilaian risiko yang meliputi identifikasi risiko, analisis risiko, dan evaluasi risiko; Perlakuan risiko; Pencatatan dan pelaporan; serta Pemantauan dan tinjauan; yang diilustrasikan pada Gambar 3 di bawah ini.

Gambar 3 – Proses manajemen risiko

Dalam proses manajemen risiko di organisasi sektor publik, pimpinan dan manajemen puncak memastikan sedikitnya:

- kepemilikan dan aktivitas proses manajemen risiko dijabarkan dan dijalankan sesuai dengan model tiga lini pertahanan; dan
- proses manajemen risiko terpadu dengan proses manajemen umum secara keseluruhan, khususnya manajemen kinerja dan sistem pengendalian internal; serta menyatu dalam budaya organisasi.

8.2 Proses komunikasi dan konsultasi

8.2.1 Proses

Sesuai SNI ISO 31000:2018 Pasal 6.2, tujuan komunikasi dan konsultasi adalah untuk membantu pemangku kepentingan yang relevan dalam memahami risiko, dasar pengambilan keputusan, dan alasan mengapa tindakan tertentu diperlukan. Komunikasi bertujuan mendorong kesadaran dan pemahaman risiko, sedangkan konsultasi mencakup pencarian umpan balik dan informasi untuk mendukung pengambilan keputusan. Koordinasi erat di antara keduanya akan memfasilitasi pertukaran informasi yang faktual, tepat waktu, relevan, akurat, dan dapat dipahami, dengan mempertimbangkan kerahasiaan dan integritas informasi, dan juga hak privasi individu.

Komunikasi dan konsultasi dengan pemangku kepentingan eksternal dan internal yang tepat sebaiknya berlangsung selama dan sepanjang seluruh tahap proses manajemen risiko.

Komunikasi dan konsultasi dimaksudkan untuk:

- menyatukan beragam area keahlian pada tiap tahap proses manajemen risiko;
- memastikan berbagai pandangan dipertimbangkan dengan memadai saat menentukan kriteria risiko dan saat mengevaluasi risiko;
- memberikan informasi yang memadai untuk memfasilitasi pengawasan risiko dan pengambilan keputusan; dan
- membangun rasa keterlibatan dan kepemilikan di antara pihak yang terpengaruh oleh risiko.

8.2.2 Bagaimana menerapkan proses komunikasi dan konsultasi pada organisasi sektor publik

Dalam proses komunikasi dan konsultasi, pimpinan dan manajemen puncak memastikan sedikitnya:

- rencana komunikasi dan konsultasi yang sistematis, terukur dan terkendali;
- metode komunikasi dan konsultasi yang tepat bagi masing-masing pemangku kepentingan; dan
- proses aktivitas komunikasi dan konsultasi terdokumentasikan sehingga dapat ditelusuri dan dijadikan rujukan.

Di bawah ini adalah langkah-langkah komunikasi dan konsultasi:

- identifikasi serta pahami harapan dan kebutuhan pemangku kepentingan;
- tentukan jenis dan metode komunikasi dan konsultasi;
- tentukan tujuan yang spesifik dalam berkomunikasi dan berkonsultasi;
- tentukan frekuensi komunikasi dan konsultasi; dan
- tetapkan pelaksana komunikasi dan konsultasi.

8.3 Proses lingkup, konteks dan kriteria

8.3.1 Proses

Sesuai SNI ISO 31000:2018 Pasal 6.3.1, tujuan penetapan ruang lingkup, konteks, dan kriteria adalah untuk menyesuaikan proses manajemen risiko, mengaktifkan penilaian risiko yang efektif dan perlakuan risiko yang memadai. Ruang lingkup, konteks, dan kriteria mencakup penentuan ruang lingkup proses dan pemahaman konteks eksternal dan internal.

Sesuai SNI ISO 31000:2018 Pasal 6.3.2, organisasi sebaiknya menentukan ruang lingkup aktivitas manajemen risikonya.

Karena proses manajemen risiko dapat diterapkan pada berbagai tingkat (misalnya strategis, operasi, program, proyek, atau aktivitas lain), diperlukan kejelasan tentang ruang lingkup yang menjadi cakupan, sasaran relevan yang perlu dipertimbangkan, dan keselarasannya dengan sasaran organisasi.

Saat merencanakan pendekatan, hal yang perlu dipertimbangkan adalah:

- sasaran dan keputusan yang perlu dibuat;
- hasil keluaran yang diharapkan dari tiap langkah yang akan diambil dalam proses;

- waktu, lokasi, serta pencakupan dan pengecualian khusus;
- alat dan teknik penilaian risiko yang sesuai;
- sumber daya yang dibutuhkan, tanggung jawab dan catatan yang disimpan; dan
- hubungan dengan proyek, proses, dan aktivitas lain.

Sesuai SNI ISO 31000:2018 Pasal 6.3.3, konteks eksternal dan internal adalah lingkungan yang dicari organisasi untuk menentukan dan mencapai sasarannya.

Konteks proses manajemen risiko sebaiknya ditetapkan dari pemahaman terhadap lingkungan eksternal dan internal tempat organisasi beroperasi serta sebaiknya merefleksikan lingkungan spesifik dari aktivitas yang menjadi sasaran penerapan manajemen risiko.

Pemahaman konteks adalah penting karena:

- manajemen risiko dilakukan dalam konteks sasaran dan aktivitas organisasi;
- faktor organisasi dapat menjadi sumber risiko; dan
- tujuan dan ruang lingkup proses manajemen risiko mungkin berhubungan dengan sasaran organisasi secara keseluruhan.

Organisasi sebaiknya menetapkan konteks eksternal dan internal proses manajemen risiko dengan mempertimbangkan faktor yang disebutkan SNI ISO 31000:2018 Pada 5.4.1.

Sesuai SNI ISO 31000:2018 Pasal 6.3.4, organisasi sebaiknya menentukan jumlah dan jenis risiko yang dapat atau tidak dapat diambil, relatif terhadap sasaran. Organisasi juga sebaiknya menentukan kriteria untuk mengevaluasi signifikansi risiko dan untuk mendukung proses pengambilan keputusan. Kriteria risiko sebaiknya selaras dengan kerangka kerja manajemen risiko dan disesuaikan dengan tujuan khusus dan ruang lingkup aktivitas yang dicakup. Kriteria risiko sebaiknya merefleksikan nilai, sasaran, dan sumber daya organisasi serta konsisten dengan kebijakan dan pernyataan tentang manajemen risiko. Kriteria sebaiknya ditentukan dengan mempertimbangkan kewajiban organisasi dan pandangan pemangku kepentingan.

Meski kriteria risiko sebaiknya ditetapkan pada awal proses penilaian risiko, kriteria itu dinamis dan sebaiknya selalu ditinjau dan disesuaikan, bila diperlukan.

Untuk menetapkan kriteria risiko, hal-hal berikut perlu dipertimbangkan:

- sifat dan jenis ketidakpastian yang dapat memengaruhi hasil keluaran dan sasaran (baik berwujud maupun tanwujud);
- bagaimana konsekuensi (baik positif maupun negatif) dan kemungkinan akan ditentukan dan diukur;
- faktor terkait waktu;
- konsistensi penggunaan ukuran;
- bagaimana tingkat risiko ditentukan;
- bagaimana kombinasi dan urutan berbagai risiko akan diperhitungkan; dan
- kapasitas organisasi.

8.3.2 Bagaimana menerapkan proses lingkup, konteks dan kriteria pada organisasi sektor publik

Dalam proses penentuan ruang lingkup, pimpinan dan manajemen puncak memastikan sedikitnya:

1) penetapan ruang lingkup manajemen risiko yang mencakupi semua sasaran dan kegiatan organisasi berdasarkan tingkat prioritas yang ditentukan secara terukur, konsisten dan sejalan dengan urgensi kebutuhan dan harapan dari pemangku kepentingan;
2) penetapan sasaran strategis di tingkat pimpinan dan manajemen puncak mencakupi tujuan berkelanjutan yang memiliki elemen sasaran ekonomis, sasaran sosial, dan sasaran lingkungan. Ketiga elemen tersebut diturunkan dan diterjemahkan ke sasaran tingkat operasional, proyek, program atau aktivitas secara proporsional dan wajar;
3) pembuatan rencana pelaksanaan manajemen risiko menyatu dengan proses perencanaan induk atau jangka panjang organisasi, dan tertaut jelas dengan perencanaan jangka pendek organisasi di tingkat operasional, proyek, program atau aktivitas. Substansi minimum yang sebaiknya ada dalam rencana pelaksanaan manajemen risiko adalah:
   - pengantar;
   - profil unit kerja sasaran, dan target kinerja;
   - sasaran pelaksanaan proses manajemen risiko;
   - kegiatan proses manajemen risiko, metode/teknik asesmen risiko yang digunakan dan keputusan penting;
   - jadwal pelaksanaan kegiatan;
   - sumber daya yang diperlukan; dan
   - evaluasi kinerja dan pelaporan.
4) penetapan kriteria konsekuensi peristiwa risiko;

   Di bawah ini adalah langkah-langkah penetapan kriteria konsekuensi:

   - identifikasi jenis-jenis efek yang paling relevan bagi organisasi. Identifikasi dapat dilakukan berdasarkan pengalaman historis, dan/atau berdasarkan studi mengenai implikasi perkembangan tuntutan dan harapan masa depan dari pemangku kepentingan terhadap capaian sasaran organisasi;
   - menentukan jumlah tingkat konsekuensi untuk menjelaskan kegawatan setiap jenis efek yang teridentifikasi; dan
   - mengembangkan pemeringkat konsekuensi untuk memberikan penjabaran mengenai setiap tingkat konsekuensi untuk setiap jenis konsekuensi.
5) penetapan kriteria kemungkinan-kejadian peristiwa risiko:

   Di bawah ini adalah langkah-langkah penyusunan kriteria kemungkinan-kejadian:

   - menentukan jumlah tingkat kemungkinan-kejadian untuk menetapkan tingkatan yang mencukupi sehingga setiap risiko dapat diberikan nilai kemungkinan-kejadian yang tepat;
   - menentukan deskripsi kemungkinan-kejadian untuk menjelaskan atribut tingkat kemungkinan-kejadian termaksud; dan
   - mengembangkan tabel kemungkinan-kejadian untuk memberikan penjabaran mengenai tingkat kemungkinan-kejadian dari setiap risiko yang teridentifikasi.

6) penetapan kriteria efektivitas kendali:

   Di bawah ini adalah langkah-langkah penyusunan kriteria efektivitas kendali:

   – menentukan skala efektivitas kendali dalam dua metrik ukuran, yaitu: apakah sistem pengendalian telah didesain dengan baik sehingga mampu mengendalikan risiko tetap berada dalam tingkat yang dapat ditoleransi; dan apakah sistem pengendalian beroperasi seperti yang diharapkan sesuai dengan desain awal; dan

   – mengembangkan pemeringkatan efektivitias kendali untuk memberikan penjabaran mengenai tingkat efektivitas kendali dari setiap pengendalian terhadap setiap risiko yang teridentifikasi.

8.4 Proses penilaian risiko

8.4.1 Proses

Sesuai SNI ISO 31000:2018 Pasal 6.4.1, penilaian risiko adalah proses menyeluruh dari identifikasi risiko, analisis risiko, dan evaluasi risiko.

Penilaian risiko sebaiknya dilakukan secara sistematis, berulang, dan kolaboratif, berdasarkan pengetahuan dan pandangan pemangku kepentingan. Penilaian sebaiknya berdasarkan informasi terbaik yang tersedia, dengan ditunjang oleh penelitian lanjutan sesuai kebutuhan.

Sesuai SNI ISO 31000:2018 Pasal 6.4.2, tujuan identifikasi risiko adalah untuk menemukan, mengenali, dan menguraikan risiko yang dapat membantu atau menghalangi organisasi dalam mencapai sasarannya. Informasi yang relevan, memadai, dan mutakhir penting dalam mengidentifikasi risiko.

Organisasi dapat memakai beragam teknik untuk mengidentifikasi ketidakpastian yang dapat memengaruhi satu atau lebih sasaran. Faktor-faktor berikut, dan hubungan antar faktor tersebut, sebaiknya dipertimbangkan:

– sumber risiko berwujud dan tanwujud;
– penyebab dan peristiwa;
– ancaman dan peluang;
– kerentanan dan kapabilitas;
– perubahan konteks eksternal dan internal;
– indikator risiko pegari (yang timbul);
– sifat dan nilai aset dan sumber daya;
– konsekuensi dan dampak terhadap sasaran;
– batasan pengetahuan dan keandalan informasi;
– faktor terkait waktu; dan
– bias, asumsi, dan kepercayaan pihak yang terlibat.

Organisasi sebaiknya mengidentifikasi risiko, tanpa memandang apakah sumber risiko itu dapat dikendalikan organisasi atau tidak. Perlu diperhatikan bahwa mungkin ada lebih dari satu jenis hasil keluaran, yang dapat menimbulkan beragam dampak berwujud atau tak berwujud.

Sesuai SNI ISO 31000:2018 Pasal 6.4.3, tujuan analisis risiko adalah untuk memahami sifat risiko dan karakteristiknya, termasuk, jika memungkinkan, tingkat risikonya. Analisis risiko melibatkan pertimbangan mendetail terhadap ketidakpastian, sumber risiko, dampak, kemungkinan, peristiwa, skenario, kendali, dan efektivitas kendali tersebut. Suatu peristiwa dapat memiliki beragam sebab dan akibat, serta dapat memengaruhi beberapa sasaran.

Analisis risiko dapat dilakukan dengan beragam tingkat detail dan kompleksitas, bergantung pada tujuan analisis, ketersediaan dan keandalan informasi, serta ketersediaan sumber daya. Teknik analisis dapat kualitatif, kuantitatif, atau kombinasi keduanya, bergantung pada kondisi dan penggunaan yang diharapkan.

Analisis risiko sebaiknya mempertimbangkan faktor seperti:

- kemungkinan peristiwa dan konsekuensi;
- sifat dan besaran konsekuensi;
- kompleksitas dan konektivitas;
- faktor dan volatilitas terkait waktu;
- efektivitas kendali yang ada; dan
- tingkat sensitivitas dan kepercayaan.

Analisis risiko dapat dipengaruhi berbagai opini yang berbeda, bias, persepsi risiko, dan penilaian. Pengaruh tambahan adalah mutu informasi yang digunakan, asumsi dan pengecualian yang dibuat, keterbatasan teknik, serta eksekusi teknik tersebut. Pengaruh tersebut sebaiknya didokumentasikan dan dikomunikasikan kepada pengambil keputusan.

Peristiwa yang ketidakpastiannya tinggi dapat sulit untuk dikuantifikasi. Hal ini dapat menjadi isu saat menganalisis peristiwa dengan konsekuensi yang parah. Pada kasus semacam itu, penggunaan kombinasi beberapa teknik secara umum dapat memberikan wawasan yang lebih luas.

Analisis risiko memberikan masukan untuk evaluasi risiko, untuk keputusan apakah risiko memerlukan perlakuan dan bagaimana perlakuannya, serta terhadap strategi dan metode perlakuan risiko yang paling sesuai. Hasilnya memberikan wawasan untuk keputusan, di mana pilihan diambil dan pilihan tersebut melibatkan berbagai jenis dan tingkat risiko.

Sesuai SNI ISO 31000:2018 Pasal 6.4.4, tujuan evaluasi risiko adalah untuk mendukung keputusan. Evaluasi risiko melibatkan pembandingan hasil analisis risiko dengan kriteria risiko yang telah ditetapkan untuk menentukan apakah diperlukan tindakan tambahan.

Hal ini dapat membawa pada keputusan untuk:

- tidak melakukan apa pun lebih lanjut;
- mempertimbangkan opsi perlakuan risiko;
- melakukan analisis lanjutan untuk memahami risiko dengan lebih baik;
- memelihara pengendalian yang ada; dan
- mempertimbangkan kembali sasaran.

Keputusan sebaiknya mempertimbangkan konteks yang lebih luas, serta konsekuensi aktual yang dipersepsikan terhadap pemangku kepentingan eksternal dan internal.

Hasil keluaran evaluasi risiko sebaiknya dicatat, dikomunikasikan, dan divalidasi pada tingkat yang tepat dalam organisasi.

8.4.2 Bagaimana menerapkan proses penilaian risiko pada organisasi sektor publik

Penilaian risiko dilakukan melalui pendekatan sistematis, yaitu:

- membuat pemetaan ketidakpastian yang relevan dengan sasaran organisasi; dan
- menjalankan tiga aktivitas berurutan yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko.

8.4.2.1 Identifikasi risiko

Identifikasi risiko dilakukan dengan cara mengidentifikasi peristiwa, penyebab, dan konsekuensi dari peristiwa risiko yang dapat menghalangi, menurunkan, atau menunda pencapaian tujuan organisasi.

Langkah-langkah proses identifikasi:

- menentukan sasaran yang akan diidentifikasi risikonya;
- menentukan hasil yang diharapkan dari setiap mata rantai tahap proses dalam mencapai sasaran;
- membuat pemetaan kondisi lingkungan internal dan eksternal yang relevan dalam pencapaian sasaran;
- mengidentifikasi setiap peristiwa risiko yang dapat dipicu oleh kondisi lingkungan; dan
- membuat register risiko.

CATATAN Sasaran sebaiknya memenuhi kriteria SMART-C (*Specific, Measureable, Attainable, Relevant, Time-bound, Challenging*).

8.4.2.2 Analisis risiko

Analisis Risiko dilakukan dengan cara menentukan tingkat konsekuensi (dampak) dan tingkat kemungkinan-kejadian terjadinya risiko berdasarkan kriteria risiko, dengan mempertimbangkan keandalan sistem pengendalian yang ada.

Langkah-langkah proses analisis risiko:

- menentukan tingkat risiko inheren dari setiap risiko yang teridentifikasi;
- menentukan tingkat keefektifan pengendalian saat ini terhadap risiko yang teridentifikasi; dan
- menentukan tingkat risiko saat ini yang diambil dari tingkat risiko inheren dengan telah memperhitungkan efektivitas kendali yang saat ini tersedia.

8.4.2.3 Evaluasi risiko

Evaluasi risiko dilakukan sebagai dasar pengambilan keputusan perlu tidaknya dilakukan upaya penanganan risiko lebih lanjut serta penentuan prioritas penanganannya.

Langkah-langkah proses evaluasi risiko:

- membandingkan tingkat risiko dari hasil analisis risiko dengan tingkat risiko yang dapat diterima, mengacu pada kriteria selera risiko (*risk appetite*) yang sudah ditetapkan sebelumnya dan mempertimbangkan ancaman yang tercermin dari tingkat risiko versus peluang yang dapat dimanfaatkan ketika risiko diambil;

- memutuskan tindak lanjut terhadap risiko. Bila tingkat risiko saat ini sesuai dengan selera risiko maka risiko dapat diterima tanpa memerlukan perlakuan risiko. Bila tingkat risiko tidak sesuai dengan selera risiko maka risiko ditolak atau menjalankan perlakuan risiko; dan
- menentukan prioritas risiko mana yang memerlukan perlakuan risiko.

8.5 Proses perlakuan risiko

8.5.1 Proses

Sesuai SNI ISO 31000:2018 Pasal 6.5.1, tujuan perlakuan risiko adalah untuk memilih dan menerapkan opsi penanganan risiko.

Perlakuan risiko mencakup proses berulang dari:

- formulasi dan seleksi opsi perlakuan risiko;
- perencanaan dan implementasi perlakuan risiko;
- penilaian efektivitas perlakuan itu;
- pengambilan keputusan apakah risiko tersisa dapat diterima; dan
- pelaksanaan perlakuan lanjutan, jika opsi tidak diterima.

Sesuai SNI ISO 31000:2018 Pasal 6.5.2, pemilihan opsi perlakuan risiko yang paling tepat mencakup penyeimbangan potensi manfaat yang diturunkan dalam kaitan dengan pencapaian sasaran terhadap biaya, upaya, atau kerugian implementasi.

Opsi perlakuan risiko tidak selalu saling berhubungan eksklusif atau tepat pada semua kondisi. Opsi perlakuan risiko dapat mencakup satu atau lebih pilihan berikut:

- menghindari risiko dengan memutuskan untuk tidak memulai atau melanjutkan aktivitas yang menimbulkan risiko;
- mengambil atau meningkatkan risiko untuk mengejar peluang;
- menghilangkan sumber risiko;
- mengubah kemungkinan;
- mengubah konsekuensi;
- membagi risiko (misalnya melalui kontrak, membeli asuransi); dan
- mempertahankan risiko dengan keputusan terinformasi.

Justifikasi untuk perlakuan risiko lebih luas daripada sekadar pertimbangan ekonomi dan sebaiknya memperhitungkan semua unsur kewajiban, komitmen sukarela, dan pandangan pemangku kepentingan dari organisasi. Pemilihan opsi perlakuan risiko sebaiknya dibuat sesuai dengan sasaran organisasi, kriteria risiko, dan sumber daya yang tersedia.

Ketika memilih opsi perlakuan risiko, organisasi sebaiknya mempertimbangkan nilai, persepsi, dan potensi keterlibatan pemangku kepentingan, serta cara paling tepat untuk berkomunikasi dan berkonsultasi dengan mereka. Meski sama-sama efektif, beberapa perlakuan risiko dapat lebih diterima oleh beberapa pemangku kepentingan dibandingkan dengan perlakuan yang lain.

Perlakuan risiko, bahkan jika sudah dirancang dan diterapkan dengan hati-hati, mungkin tidak mencapai hasil keluaran yang diharapkan dan dapat memberi konsekuensi yang tidak diharapkan. Pemantauan dan tinjauan perlu menjadi bagian integral implementasi perlakuan risiko untuk memberi pemastian bahwa berbagai bentuk perlakuan menjadi dan tetap efektif.

Perlakuan risiko juga dapat menimbulkan risiko baru yang perlu dikelola.

Jika opsi perlakuan risiko tidak tersedia atau jika opsi perlakuan tidak mengubah risiko secara memadai, risiko tersebut sebaiknya dicatat dan terus ditinjau.

Pengambil keputusan dan pemangku kepentingan lain sebaiknya menyadari sifat dan jangkauan risiko yang tersisa setelah perlakuan risiko. Risiko yang tersisa sebaiknya didokumentasikan dan menjadi subjek pemantauan, tinjauan, dan, bila diperlukan, perlakuan lanjutan.

Sesuai SNI ISO 31000:2018 Pasal 6.5.3, tujuan rencana perlakuan risiko adalah untuk menentukan bagaimana opsi perlakuan yang dipilih dapat diterapkan, sehingga pengaturannya dapat dipahami oleh pihak yang terlibat dan kemajuan rencananya dapat dipantau.

Rencana perlakuan sebaiknya jelas mengidentifikasi urutan perlakuan risiko yang sebaiknya diterapkan.

Rencana perlakuan sebaiknya terintegrasi dengan rencana dan proses manajemen organisasi, melalui konsultasi dengan pemangku kepentingan yang sesuai.

Informasi yang diberikan di dalam rencana perlakuan sebaiknya mencakupi:

- alasan pemilihan opsi perlakuan, termasuk manfaat yang diharapkan;
- pihak yang memiliki akuntabilitas dan tanggung jawab untuk persetujuan dan implementasi rencana;
- tindakan yang diusulkan;
- sumber daya yang dibutuhkan, termasuk kontingensi;
- ukuran kinerja;
- batasan;
- pelaporan dan pemantauan yang diperlukan; dan
- kapan tindakan diharapkan dapat dilakukan dan diselesaikan.

8.5.2 Bagaimana menerapkan proses perlakuan risiko pada organisasi sektor publik

Perlakuan risiko diperlukan untuk menurunkan tingkat risiko sampai setidaknya di tingkat selera risiko yang telah ditentukan. Perlakuan risiko dapat dilakukan dengan menurunkan (*reduce*) tingkat kemungkinan-kejadian suatu peristiwa risiko, dan/atau menurunkan tingkat dampak (*mitigate*) dari peristiwa risiko tersebut.

Langkah-langkah perlakuan risiko:

- mengidentifikasi opsi perlakuan risiko yang dapat dilakukan;
- membandingkan opsi perlakuan risiko yang tersedia melalui analisis manfaat-biaya;
- memilih opsi perlakuan risiko yang patut dan layak;
- merencanakan implementasi opsi perlakuan risiko yang terpilih;

- menerapkan perlakuan risiko sesuai rencana implementasi;
- menilai keefektifan perlakuan risiko yang telah diterapkan; dan
- memutuskan apakah tingkat risiko tersisa (*residual risk*) setelah perlakuan risiko sudah sesuai dengan selera risiko. Jika tidak, terapkan perlakuan risiko lanjutan.

8.6 Proses pemantauan dan tinjauan

8.6.1 Proses

Sesuai SNI ISO 31000:2018 Pasal 6.6, tujuan pemantauan dan tinjauan kembali adalah untuk memastikan dan meningkatkan mutu dan efektivitas desain, implementasi, dan hasil keluaran proses. Pemantauan yang sedang berlangsung dan tinjauan berkala terhadap proses dan hasil keluaran manajemen risiko sebaiknya menjadi bagian terencana dari proses manajemen risiko, dengan tanggung jawab yang ditentukan dengan jelas.

Pemantauan dan tinjauan sebaiknya dilaksanakan pada semua tahap proses. Pemantauan dan tinjauan mencakup perencanaan, pengumpulan dan analisis informasi, pencatatan hasil, dan pemberian umpan balik.

Hasil pemantauan dan tinjauan sebaiknya disertakan di seluruh aktivitas manajemen, pengukuran, dan pelaporan kinerja organisasi.

8.6.2 Bagaimana menerapkan proses pemantauan dan tinjauan pada organisasi sektor publik

Pemantauan dan tinjauan dilakukan terhadap seluruh aspek pelaksanaan proses manajemen risiko, dengan memperhatikan hal-hal sebagai berikut:

- keefektifan indikator risiko yang digunakan untuk memantau gejala keterjadian risiko;
- mekanisme untuk memperoleh data indikator risiko terjamin efisiensinya dan pihak yang menjadi sumber data telah terkomunikasi dan siap mendukung pasokan data sesuai kebutuhan;
- batasan kemungkinan-kejadian keterjadian risiko (*risk treshold*), baik batas atas (*upper treshold*) dan batas bawah (*lower treshold*) telah ditetapkan melalui pertimbangan yang matang sehingga efektif untuk memantau gejala (*trend*) keterjadian risiko; dan
- jadwal pemantauan ditetapkan dengan mempertimbangkan kondisi beban kerja pemantau dan kebutuhan akurasi pemantauan.

Peninjauan dilakukan dalam bentuk evaluasi terhadap proses manajemen risiko dengan fokus, sedikitnya pada:

- kepatuhan; jika catatan hasil pemantauan menunjukkan terjadi ketidaksesuaian antara pelaksanaan tahapan proses manajemen risiko dengan ketentuan yang seharusnya, maka dilakukan evaluasi untuk mengetahui sumber penyebabnya dan kemudian dibuatkan rekomendasi perbaikannya;
- keefektifan; jika catatan hasil pemantauan menunjukkan terjadi deviasi antara target versus aktual pada setiap tahap proses manajemen risiko maka dilakukan evaluasi untuk mengetahui sumber penyebabnya dan kemudian dibuatkan rekomendasi perbaikannya; dan

- perubahan lingkungan; jika catatan hasil pemantauan menunjukkan terjadi perubahan lingkungan yang diduga dapat menurunkan keefektifan pelaksanaan setiap tahap dalam proses manajemen risiko termasuk keefektifan perlakuan risiko, maka dilakukan evaluasi untuk mengetahui sumber penyebabnya dan kemudian dibuatkan rekomendasi perbaikannya.

8.7 Proses pencatatan dan pelaporan

8.7.1 Proses

Sesuai SNI ISO 31000:2018 Pasal 6.7, proses dan hasil keluaran manajemen risiko sebaiknya didokumentasikan dan dilaporkan melalui mekanisme yang sesuai. Pencatatan dan pelaporan bertujuan untuk:

- mengomunikasikan aktivitas manajemen risiko dan hasil keluaran dari manajemen risiko ke seluruh organisasi;
- memberikan informasi untuk pengambilan keputusan;
- meningkatkan aktivitas manajemen risiko; dan
- membantu interaksi dengan pemangku kepentingan, termasuk pihak yang memiliki tanggung jawab dan akuntabilitas untuk aktivitas manajemen risiko.

Keputusan yang berkaitan dengan pembuatan, retensi, dan penanganan informasi terdokumentasi sebaiknya mempertimbangkan, tetapi tidak terbatas pada, penggunaannya, sensitivitas informasi, serta konteks eksternal dan internal.

Pelaporan adalah bagian integral dari tata kelola organisasi dan sebaiknya meningkatkan mutu dialog dengan pemangku kepentingan dan mendukung manajemen puncak dan badan pengawas dalam memenuhi tanggung jawab mereka. Faktor yang perlu dipertimbangkan dalam pelaporan mencakup, tetapi tidak terbatas pada:

- berbagai perbedaan pemangku kepentingan yang berbeda serta kebutuhan dan persyaratan informasi mereka yang khusus;
- biaya, frekuensi, dan ketepatan waktu pelaporan;
- metode pelaporan; dan
- relevansi informasi terhadap sasaran dan pengambilan keputusan organisasi.

8.7.2 Bagaimana menerapkan proses pencatatan dan pelaporan pada organisasi sektor publik

Pimpinan dan manajemen puncak sebaiknya memastikan sistem pencatatan dan pelaporan sedikitnya:

- mampu mendukung pengambilan keputusan di tingkat pimpinan dan manajemen puncak, serta di setiap pemilik risiko dalam organisasi sesuai dengan hirarki fungsi dan peran masing-masing;
- dijalankan di setiap tahapan proses manajemen risiko, mulai dari komunikasi dan konsultasi dengan pemangku kepentingan terkait penilaian risiko, perlakuan risiko, sampai dengan tahapan pemantauan dan tinjauan;
- menjadi bagian terpadu dari laporan akuntabilitas pimpinan dan manajemen puncak, terutama dalam pertanggungjawaban kinerja mereka untuk capaian sasaran strategis di tingkat lembaga; dan
- tersedia secara teratur, dan terbuka bagi pemangku kepentingan yang relevan.

Lampiran A
(informatif)
Contoh peta jalan pengimplementasian manajemen risiko

Tabel A.1 – Contoh peta jalan pengimplementasian manajemen risiko

Manajemen risiko
menciptakan dan melindungi nilai

Tahapan / Unsur	Membangun infrastruktur	Membangun kapasitas	Mengintegrasikan manajemen risiko	Membangun budaya sadar risiko
Kegiatan	• Membuat kebijakan manajemen risiko • Membuat pedoman manajemen risiko • Membuat prosedur dan manual manajemen risiko • Membentuk unit manajemen risiko • Menentukan pengelola risiko pada satuan kerja operasional • Membangun infrastruktur fisik	• Pengarahan eksekutif bagi pimpinan organisasi mengenai tata kelola risiko • Penyediaan pelatihan kompetensi manajemen risiko bagi pelaksana organisasi pada berbagai tingkatan (dapat di koordinasikan oleh *Human Resource Department*) • Penyediaan pelatihan kompetensi manajemen risiko bagi pengawas internal (dapat di koordinasikan oleh *Human Resource Department*) • Pengembangan Sistem Informasi Manajemen Risiko (SIM-Risiko)	• Integrasi manajemen risiko ke dalam proses perencanaan strategis dan penganggaran • Integrasi manajemen risiko ke dalam proses bisnis utama organisasi • Integrasi manajemen risiko ke dalam proses pengawasan internal • Integrasi manajemen risiko ke dalam proses pengelolaan proyek • Integrasi manajemen risiko ke dalam proses bisnis penunjang (misal: Teknologi Informasi, Sumber Daya Manusia, dsb)	• Asesmen budaya sadar risiko • Program dan pelatihan budaya sadar risiko • Penerapan manajemen risiko merupakan bagian dari penilaian kinerja
Keluaran	• Terbentuknya tata kelola manajemen risiko • Kejelasan peran dan tanggung jawab penerapan manajemen risiko: √ Lini pertama √ Lini kedua √ Lini ketiga	• Pimpinan organisasi memahami tata kelola risiko • Pelaksana organisasi memiliki kompetensi memadai bidang manajemen risiko • Pengawas internal memiliki kompetensi memadai bidang manajemen risiko • SIM-Risiko berfungsi dengan baik dan mendukung penerapan manajemen risiko secara keseluruhan	• Perencanaan strategis berbasis risiko • Penganggaran berbasis risiko • Proses bisnis utama berbasis risiko • Pengawasan internal berbasis risisko • Proses pengelolaan proyek berbasis risiko • Proses bisnis penunjang berbasis risiko • Pengambilan keputusan berbasis risiko	• Meningkatnya kesadaran bahwa risiko merupakan bagian tak terpisahkan dalam kehidupan organisasi • Perilaku organisasi dan individu yang positif terhadap risiko
Hasil	Kesiapan untuk implementasi manajemen risiko di seluruh organisasi	Implementasi manajemen risiko memberikan manfaat berdasarkan kebutuhan dan bukan semata-mata karena kepatuhan	Manajemen risiko menjadi bagian terpadu (integral) dengan keseluruhan proses dalam organisasi	Budaya sadar risiko menjadi budaya organisasi dan terinternalisasi pada setiap orang dalam organisasi sehingga tumbuh kesadaran tanggung jawab manajemen risiko pada masing-masing individu

	Monitoring dan reviu	Monitoring dan reviu	Monitoring dan reviu	Monitoring dan reviu

Pengembangan dan penerapan manajemen risiko secara berkelanjutan dan penilaian tingkat maturitas

Lampiran B
(informatif)
Contoh pembentukan struktur manajemen risiko

B.1 Umum

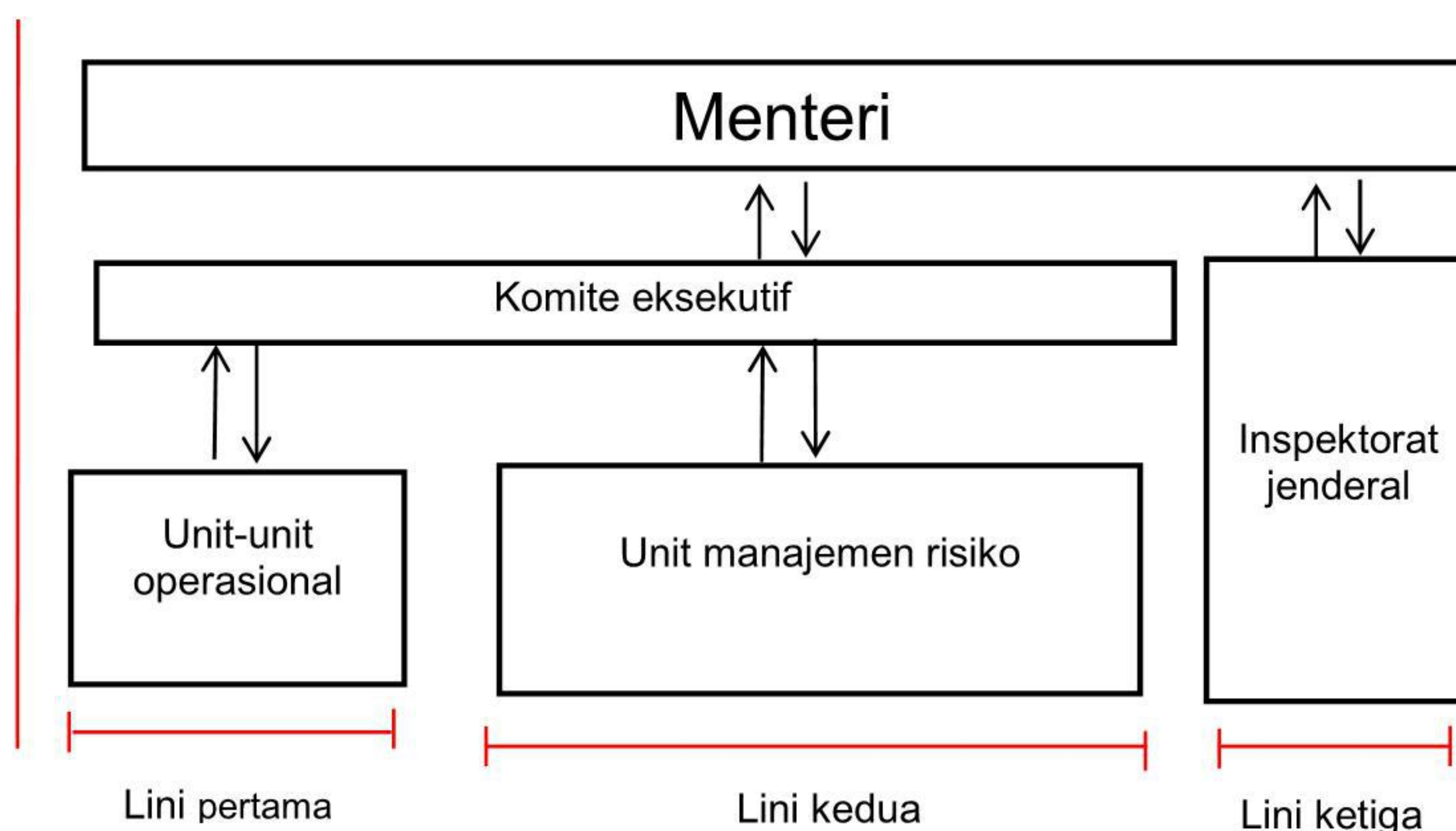
Struktur manajemen risiko ditetapkan oleh organ tertinggi organisasi sektor publik bersangkutan agar pengendalian dan pengawasan pengendalian terhadap penerapan manajemen risiko terjalankan dengan efektif dan efisien bagi lembaga tersebut.

CATATAN Lampiran ini adalah contoh bagaimana struktur oganisasi manajemen risiko di lembaga kementerian. Pembentukan struktur di organisasi sektor publik lain perlu disesuaikan dengan payung hukum dan regulasi yang berlaku bagi lembaga tersebut.

B.2 Struktur manajemen risiko di lembaga kementerian

Sebagai organ tertinggi lembaga kementerian bersangkutan, menteri bertugas untuk menetapkan struktur manajemen risiko lembaga yang mencerminkan penerapan model tiga lini pertahanan dan terdiri dari sedikitnya:

– komite manajemen risiko di tingkat lembaga, disebut sebagai komite eksekutif dan diketuai oleh menteri;
– unit-unit operasional yang berfungsi sebagai lini pertama pertahanan;
– unit manajemen risiko sebagai lini kedua pertahanan; dan
– inspektorat jenderal sebagai lini ketiga pertahanan.

Gambar di bawah ini adalah ilustrasi model tiga lini pertahanan di lembaga kementerian.

Gambar B.1 – Contoh struktur manajemen risiko di lembaga kementerian

CATATAN Bagi organisasi sektor publik non lembaga kementerian perlu menyesuaikan dengan konteks masing-masing, termasuk nomenklatur yang digunakan.

B.2.1 Tugas dan tanggung jawab komite eksekutif

a) menetapkan kebijakan dan pedoman manajemen risiko kementerian;

b) menetapkan profil risiko kunci kementerian beserta dengan rencana mitigasinya berdasarkan sasaran strategis kementerian secara tahunan;

c) menetapkan selera risiko (*risk appetite*) dan kriteria risiko yang berlaku di kementerian;

d) melakukan reviu dan evaluasi terhadap implementasi manajemen risiko di kementerian; dan

e) memastikan bahwa implementasi manajemen risiko berjalan efektif di kementerian.

B.2.2 Tugas dan tanggung jawab unit-unit operasional

a) menentukan sasaran dan program manajemen risiko pada unit-unit operasional di tingkat JPT Madya;

b) menyusun dan menetapkan risiko-risiko kunci pada unit-unit operasional di tingkat JPT Madya dan risiko-risiko kunci unit-unit operasional di bawahnya (di tingkat JPT Pratama), terutama yang berkarakteristik sama atau homogen;

c) menyusun, menetapkan, dan melaporkan (kepada komite eksekutif) profil risiko kunci pada unit-unit operasional di tingkat JPT Madya beserta rencana mitigasinya berdasarkan sasaran strategis unit-unit operasional tersebut secara tahunan;

d) menginformasikan risiko-risiko kunci kementerian pada unit-unit operasional di tingkat JPT Madya, dan di tingkat bawahnya (di tingkat JPT Pratama) yang homogen serta rencana mitigasi yang relevan kepada seluruh unit-unit operasional di bawahnya;

e) memantau dan melaporkan (kepada komite eksekutif) tingkat aktual risiko kunci pada unit-unit operasional di tingkat JPT Madya serta pelaksanaan mitigasi risiko kunci lembaga kementerian pada unit-unit operasional tersebut;

f) menelaah rekomendasi dari inspektorat jenderal kepada unit-unit operasional bersangkutan dan menentukan tindak lanjutnya;

g) memastikan bahwa proses manajemen risiko berjalan efektif pada unit-unit operasional di tingkat JPT Madya dan unit-unit operasional di bawahnya (di tingkat JPT Pratama); dan

h) memberikan masukan/rekomendasi kepada pemimpin unit-unit operasional di tingkat JPT Madya berdasarkan suatu analisis objektif berkenaan dengan pengambilan keputusan/kebijakan yang sesuai dengan permintaan pemimpin pada unit-unit operasional tersebut.

B.2.3 Tugas dan tanggung jawab unit manajemen risiko

a) menyusun kebijakan dan pedoman manajemen risiko kementerian sebagai pedoman penerapan manajemen risiko bagi seluruh unit di lingkungan kementerian;

b) menyusun profil risiko kunci kementerian dan rencana mitigasinya berdasarkan sasaran strategis kementerian secara tahunan;

c) memantau dan melaporkan (kepada komite eksekutif) tingkat aktual risiko kunci kementerian dan pelaksanaan mitigasinya;

d) menginformasikan risiko-risiko kunci kementerian serta menyampaikan rencana mitigasi kementerian yang relevan kepada seluruh unit-unit operasional di tingkat JPT Madya yang terkait;

e) memberikan masukan kepada menteri melalui komite eksekutif tentang rencana kontinjensi apabila kondisi eksternal yang tidak normal terjadi;

f) memberikan masukan/rekomendasi kepada menteri melalui komite eksekutif berdasarkan suatu analisis objektif berkenaan dengan pengambilan keputusan/kebijakan menteri tertentu sesuai permintaan menteri.

g) memantau secara berkala penyelesaian atau penanganan profil risiko kunci beserta dengan rencana mitigasi risiko sesuai dengan unit kerjanya; dan

h) melakukan pemantauan pelaksanaan rencana mitigasi risiko sesuai dengan unit kerjanya.

CATATAN Unit Manajemen Risiko (UMR) dengan tugas dan tanggung jawab di atas dapat dibentuk sebagai unit tersendiri, atau dipadukan dengan Unit Kepatuhan Internal (UKI), atau penugasan kepada UKI tergantung kebutuhan organisasi bersangkutan.

B.2.4 Tugas dan tanggung jawab inspektorat jenderal

Memastikan pelaksanaan tugas dan tanggung jawab di bawah ini berdasarkan asas independensi:

a) pemantauan dan reviu atas proses manajemen risiko pada lembaga kementerian, dan pada unit-unit operasional baik di tingkat JPT Madya, maupun di tingkat JPT Pratama;

b) penilaian atas tingkat maturitas risiko pada lembaga kementerian, dan pada unit-unit operasional baik di tingkat JPT Madya, maupun di tingkat JPT Pratama;

c) audit atas proses manajemen risiko pada lembaga kementerian, dan pada unit-unit operasional baik di tingkat JPT Madya, maupun di tingkat JPT Pratama; dan

d) pemberian jasa konsultasi dan asistensi atas penerapan manajemen risiko di lingkungan lembaga kementerian.

Lampiran C
(informatif)
Contoh kebijakan manajemen risiko

Kebijakan manajemen risiko di bawah ini adalah **contoh** bagi organisasi sektor publik berbentuk lembaga kementerian.

CATATAN Bagi organisasi sektor publik non lembaga kementerian perlu menyesuaikan dengan konteks masing-masing, termasuk nomenklatur yang digunakan.

Secara umum, kebijakan manajemen risiko lembaga meliputi:

1) Kebijakan skala risiko lembaga

Tingkat risiko ditentukan berdasarkan atas dua elemen, yaitu tingkat kemungkinan-kejadian terjadinya risiko dan tingkat konsekuensi risiko. Kedua dimensi tersebut sebaiknya dikombinasikan dan diperhitungkan secara bersamaan dalam penentuan **Tingkat Risiko.**

Tingkat kemungkinan-kejadian dan tingkat konsekuensi masing-masing menggunakan lima skala tingkatan, yang disajikan dalam bentuk matriks analisis risiko sebagaimana ditampilkan dalam bentuk tabel C.1. Dalam tabel tersebut juga tersajikan **Besaran Risiko** yang merupakan hasil perkalian skala tingkat konsekuensi dan skala kemungkinan-kejadian yang terkait. Di bawah ini adalah ilustrasi tabel C.1 secara keseluruhan.

Tabel C.1 – Contoh matriks analisis risiko – Peta besaran risiko (5x5)

Tingkat kemungkinan -kejadian \ **Tingkat konsekuensi**		1	2	3	4	5
		Tidak signifikan	Minor	Moderat	Signifikan	Sangat signifikan
5	Hampir pasti terjadi	5	10	15	20	25
4	Sering terjadi	4	8	12	16	20
3	Kadang terjadi	3	6	9	12	15
2	Jarang terjadi	2	4	6	8	10
1	Hampir tidak terjadi	1	2	3	4	5

CATATAN 1

CATATAN 1 Bila organisasi menghadapi dua risiko dengan besaran risiko yang sama tetapi memiliki kombinasi berbeda, misal besaran risiko 20 dimana yang satu terdiri dari tingkat kemungkinan-kejadian 4 dan konsekuensi 5, dan yang lain terdiri dari tingkat kemungkinan kejadian 5 dan konsekuensi 4; organisasi sebaiknya memberikan prioritas risiko yang sama terhadap keduanya. Namun ketika organisasi terpaksa harus memberikan prioritas berbeda, sebaiknya besaran risiko dengan konsekuensi yang lebih besar diberikan prioritas yang lebih tinggi.

Melalui matriks analisis risiko dapat diketahui urutan **Besaran Risiko**. Pada tabel C.2 menunjukkan Besaran risiko yang dikelompokan berdasarkan tingkat risiko dan prioritas risiko kedalam lima tingkatan yaitu:

- tingkat sangat tinggi atau lima;
- tingkat tinggi atau empat;
- tingkat sedang atau tiga;
- tingkat rendah atau dua; dan
- tingkat sangat rendah atau satu.

Tabel C.2 – Contoh matriks analisis risiko – Penentuan prioritas risiko

Besaran risiko		Prioritas risiko	Tingkatan	Tingkat risiko
Numerik	Warna			
25		1	5	Sangat tinggi
24		2		
23		3		
22		4	4	Tinggi
21		5		
20		6		
19		7		
18		8		
17		9	3	Sedang
16		10		
15		11		
14		12		
13		13		
12		14		
11		15		
10		16		
9		17		
8		18	2	Rendah
7		19		
6		20		
5		21		
4		22		
3		23	1	Sangat rendah
2		24		
1		25		
CATATAN Pewarnaan besaran risiko hanya untuk membantu visualisasi.				

2) Kriteria risiko lembaga

Kriteria risiko merupakan parameter atau ukuran, baik secara kuantitatif maupun kualitatif, yang digunakan untuk menentukan tingkat kemungkinan-kejadian terjadinya risiko dan tingkat konsekuensi atas suatu risiko. Penentuan kriteria risiko sebaiknya memerhatikan regulasi yang ada dan aspirasi pemangku kepentingan.

Penyusunan kriteria ini menjadi bagian penting yang akan digunakan pada langkah analisis Risiko. Kriteria yang perlu dibuat antara lain:

- Kriteria kemungkinan-kejadian terjadinya Risiko (*likelihood/frequency*), yaitu besarnya peluang atau frekuensi suatu Risiko akan terjadi. Pengukurannya bisa menggunakan pendekatan statistik (*probability*), frekuensi peristiwa persatuan waktu (hari, minggu, bulan, tahun), atau dengan *expert judgement*. Contoh kriteria kemungkinan-kejadian sebagaimana terdapat pada tabel C.3 di bawah.

- Kriteria konsekuensi (*consequences*), yaitu area konsekuensi apa saja yang perlu dijadikan kriteria untuk penilaian tinggi rendahnya akibat dari suatu Risiko, misalnya kerugian finansial, penurunan reputasi, penurunan kinerja, tuntutan hukum, dan lain-lain. Contoh kriteria konsekuensi sebagaimana terdapat pada tabel C.4.

Unit manajemen risiko bertugas untuk menyusun kriteria Risiko yang seragam. Kemudian kriteria tersebut disampaikan kepada komite eksekutif untuk dibahas dan ditetapkan oleh menteri.

Tabel C.3 – Contoh kriteria kemungkinan-kejadian

Tingkat kemungkinan-kejadian	Kriteria kemungkinan-kejadian
Hampir tidak terjadi (1)	➢ Kemungkinan terjadinya sangat jarang (kurang dari … kali dalam … tahun). ➢ Persentase kemungkinan terjadinya kurang dari …% dalam … periode.
Jarang terjadi (2)	➢ Kemungkinan terjadinya jarang (… kali s.d. … kali dalam … tahun). ➢ Persentase kemungkinan terjadinya …% s.d. …% dalam … periode.
Kadang terjadi (3)	➢ Kemungkinan terjadinya cukup sering (di atas … kali s.d. … kali dalam … tahun). ➢ Persentase kemungkinan terjadinya di atas …% s.d. …% dalam … periode.
Sering terjadi (4)	➢ Kemungkinan terjadinya sering (di atas … kali s.d. … kali dalam … tahun). ➢ Persentase kemungkinan terjadinya di atas …% s.d. …% dalam … periode.
Hampir pasti terjadi (5)	➢ Kemungkinan terjadinya sangat sering (di atas … kali dalam … tahun). ➢ Persentase kemungkinan terjadinya lebih dari …% dalam … periode.

CATATAN 1 Dalam merancang kriteria, setiap organisasi tidak harus menggunakan deskripsi kriteria yang sama. Dengan demikian, organisasi dapat mengisi (…) yang sudah disesuaikan dengan konteks organisasi.

CATATAN 2 Terpenting adalah kriteria terdiri dari lima tingkatan dan konsisten dalam ukuran yang dipakai serta pelaksanaannya.

Tabel C.4 – Contoh kriteria konsekuensi

Tingkat konsekuensi	Area konsekuensi				
	Kerugian negara	**Penurunan reputasi**	**Penurunan kinerja**	**Gangguan terhadap layanan organisasi**	**Tuntutan hukum**
Tidak Signifikan (1)	Jumlah kerugian negara ≤ Rp. …	Keluhan pemangku kepentingan secara langsung lisan/tertulis ke organisasi jumlahnya ≤ … dalam satu periode	Pencapaian target kinerja ≤ …%	Pelayanan tertunda ≤ … hari	Jumlah tuntutan hukum ≤ … kali dalam satu periode
Minor (2)	Jumlah kerugian negara dari Rp… s.d. Rp…	Keluhan pemangku kepentingan secara langsung lisan/tertulis ke organisasi jumlahnya lebih dari … dalam satu periode	Pencapaian target kinerja di atas …% s.d. …%	Pelayanan tertunda di atas … hari s.d. … hari	Jumlah tuntutan hukum di atas … s.d. … kali dalam satu periode
Moderat (3)	Jumlah kerugian negara dari Rp… s.d. Rp…	Pemberitaan negatif di media massa lokal	Pencapaian target kinerja di atas …% s.d. …%	Pelayanan tertunda di atas … hari s.d. … hari	Jumlah tuntutan hukum di atas … s.d. … kali dalam satu periode
Signifikan (4)	Jumlah kerugian negara lebih dari Rp… s.d. Rp…	Pemberitaan negatif di media massa nasional	Pencapaian target kinerja di atas …% s.d. …%	Pelayanan tertunda di atas … hari s.d. … hari	Jumlah tuntutan hukum di atas … s.d. … kali dalam satu periode
Sangat Signifikan (5)	Jumlah kerugian negara lebih dari Rp…	Pemberitaan negatif di media massa internasional	Pencapaian target kinerja	Pelayanan tertunda lebih dari … hari	Jumlah tuntutan hukum lebih dari … kali dalam satu periode

CATATAN 1 Dalam merancang konsekuensi, setiap organisasi tidak harus menggunakan deskripsi konsekuensi yang sama. Dengan demikian, organisasi dapat mengisi (…) yang sudah disesuaikan dengan konteks organisasi.

CATATAN 2 Terpenting adalah konsekuensi terdiri dari lima tingkatan dan konsisten dalam ukuran yang dipakai serta pelaksanaannya.

3) Kategori risiko

Tabel C.5 – Contoh kategori risiko

No	Kategori risiko	Definisi
1	Risiko penerimaan	Risiko yang disebabkan oleh tidak tercapainya target penerimaan negara yang diamanahkan ke organisasi.
2	Risiko belanja	Risiko yang disebabkan oleh kegagalan organisasi dalam penyerapan belanja negara yang tidak sesuai proyeksi. (proporsionalitas penyerapan), atau tidak sesuai dengan sasaran penggunaan.
3	Risiko pembiayaan	Risiko yang disebabkan oleh kegagalan organisasi dalam pemenuhan pembiayaan, baik nominal maupun jadwal waktunya.
4	Risiko strategi	Risiko yang disebabkan oleh ketidaktepatan organisasi dalam mengambil keputusan memilih strategi, ketidaktepatan atau tidak dilaksanakannya suatu keputusan strategis, serta kegagalan dalam mengantisipasi perubahan lingkungan berupa perubahan kondisi sosial, politik, dan ekonomi.
5	Risiko *fraud*	Risiko yang disebabkan oleh kecurangan yang disengaja yang merugikan keuangan negara. *Fraud* meliputi: penggelapan aset (barang milik negara atau kas dan setara kas), korupsi (suap-menyuap, gratifikasi, dan lain-lain) serta manipulasi laporan kinerja dan keuangan.
6	Risiko kepatuhan	Risiko yang disebabkan oleh kejadian dimana organisasi tidak mematuhi dan/atau tidak melaksanakan peraturan perundang-undangan dan ketentuan yang berlaku. Sumber risiko kepatuhan antara lain timbul karena kurangnya pemahaman atau kesadaran hukum terhadap ketentuan maupun peraturan perundang-undangan yang berlaku umum.
7	Risiko operasional	Risiko yang disebabkan karena: - ketidakcukupan dan/atau tidak berfungsinya proses internal, kesalahan manusia dan kegagalan sistem; - adanya kejadian eksternal yang memengaruhi operasional organisasi; - adanya tuntutan hukum dari luar kepada organisasi.
8	Risiko reputasi	Risiko yang disebabkan oleh menurunnya tingkat kepercayaan pemangku kepentingan eksternal yang bersumber dari persepsi negatif terhadap organisasi.

CATATAN Dalam merancang kategori risiko, setiap organisasi tidak harus menggunakan jumlah dan jenis kategori yang sama. Hal ini tergantung oleh tingkat atau ukuran setiap sektor publik.

4) Selera risiko lembaga

Selera risiko lembaga harus dipersiapkan oleh komite eksekutif untuk dibahas dan ditetapkan oleh menteri. Di bawah ini contoh bagaimana selera risiko ditentukan sebagai ambang besaran risiko (*threshold*) yang sebaiknya dimitigasi.

Tabel C.6 – Contoh selera risiko

No	Kategori risiko	Besaran risiko yang sebaiknya dimitigasi
1	Risiko penerimaan	≥10
2	Risiko belanja	≥10
3	Risiko pembiayaan	≥10
4	Risiko strategis	≥ 9
5	Risiko *fraud*	≥ 4
6	Risiko kepatuhan	≥ 9
7	Risiko operasional	≥ 15
8	Risiko reputasi	≥ 15

CATATAN 1 Jika besaran risiko berada di atas batas ambang yang telah ditetapkan maka organisasi perlu melakukan mitigasi risiko.

CATATAN 2 Penggunaan angka ambang di bawah ini hanya diberikan untuk kebutuhan ilustrasi. Dalam implementasi, sesungguhnya organisasi perlu menentukan ambang besaran risiko per kategori yang relevan dengan konteks mereka masing-masing.

Di bawah ini adalah ilustrasi selera risiko di lembaga kementerian.

Ambang ≥ 10

Risiko penerimaan
Tingkat Kemungkinan-Kejadian
Tingkat Konsekuensi
Ambang ≥ 10
Risiko belanja
Tingkat Kemungkinan-Kejadian
Tingkat Konsekuensi
Ambang ≥ 10
Risiko pembiayaan
Tingkat Kemungkinan-Kejadian
Tingkat Konsekuensi
Ambang ≥ 10
Risiko strategis
Tingkat Kemungkinan-Kejadian
Tingkat Konsekuensi
Ambang ≥ 9
Risiko fraud
Tingkat Kemungkinan-Kejadian
Tingkat Konsekuensi
Ambang ≥ 4
Risiko kepatuhan
Tingkat Kemungkinan-Kejadian
Tingkat Konsekuensi
Ambang ≥ 9

Ambang ≥ 15

Ambang ≥ 15

CATATAN 1 (- - -) dalam ilustrasi di atas menggambarkan garis selera risiko dengan ambang besaran risiko (*threshold*) yang sebaiknya dimitigasi.

CATATAN 2 Risiko yang berada di garis tersebut dan di atasnya adalah risiko yang memerlukan perlakuan risiko.

Lampiran D
(informatif)
Contoh pengembangan budaya sadar risiko

D.1 Umum

Budaya sadar risiko penting dalam implementasi manajemen risiko karena memengaruhi kapabilitas organisasi mulai dari mengambil keputusan strategis sampai dengan menjalankan keputusan tersebut secara efisien dan efektif di tingkat operasional. Budaya tersebut perlu dibangun, dikembangkan, disebarkan, dan diperkuat dari waktu ke waktu agar tercipta kepedulian dan kepemilikan risiko di seluruh jajaran organisasi.

Dengan adanya budaya sadar risiko, kepedulian dan kepemilikan risiko, organisasi dapat mendorong, memampukan dan menghargai baik para individu maupun kelompok-kelompok untuk mengambil risiko yang tepat dan mengelolanya sedemikian rupa sehingga organisasi dapat memiliki tingkat kemungkinan sukses yang lebih tinggi dalam pencapaian sasaran mereka.

D.2 Tahapan pengembangan budaya sadar risiko

Dalam rangka menciptakan budaya sadar risiko, ada berbagai inisiatif yang perlu dilakukan oleh organisasi. Di bawah ini adalah contoh delapan inisiatif yang sedikitnya perlu dilakukan dalam membangun budaya sadar risiko:

Gambar D.1 – Inisiatif pengembangan budaya sadar risiko

Komitmen pimpinan organisasi sektor publik

Komitmen pimpinan organisasi dan manajemen puncak dalam menciptakan irama sama (*tone at the top*) dengan selalu mempertimbangkan risiko dalam setiap pengambilan keputusan dan tindakan. Pimpinan adalah pendorong utama memulai budaya sadar risiko yang dilanjutkan oleh peran semua manajemen puncak dan menengah dalam mengomunikasikan dan memengaruhi perilaku seluruh karyawan dalam penerapan manajemen risiko. Komitmen pimpinan ditunjukkan antara lain dengan memastikan bahwa sumber daya organisasi tersedia secara memadai bagi penerapan manajemen risiko.

Edukasi

Pemberian edukasi kepada seluruh pemangku kepentingan mengenai pentingnya manajemen risiko, terutama pelatihan dan pengembangan kompetensi bidang manajemen risiko yang relevan dan terkait dengan penerapan SNI ISO 31000:2018. Pelatihan dan pengembangan kompetensi bidang manajemen risiko diberikan kepada pegawai di seluruh tingkatan organisasi dan kepada mitra eksternal organisasi yang terlibat dalam proses bisnis mereka sehingga irama dan standar proses manajemen risiko antara organisasi dengan mitranya dapat tersinkronisasi.

Praktik

Penyelenggaraan berbagai kegiatan untuk berbagi pengetahuan dan pengalaman mengenai manajemen risiko, baik antar karyawan dalam organisasi ataupun antar organisasi dengan organisasi lainnya. Kegiatan berbagi pengetahuan dan pengalaman tersebut dimaksudkan untuk pengembangan dan/atau penguatan kompetensi internal kolektif dalam pengelolaan risiko.

Komunikasi

Komunikasi berkelanjutan mengenai pentingnya manajemen risiko dijalankan secara konsisten kepada seluruh jajaran organisasi, baik dalam rapat-rapat pengambilan keputusan maupun dalam pertemuan-pertemuan yang terkait dengan pelaksanaan proses manajemen risiko. Profil dan peta risiko serta rancangan mitigasi risiko yang telah tersusun sebaiknya dikomunikasikan kepada semua anggota organisasi untuk mendapatkan dukungan dan keterlibatan mereka dalam pelaksanaannya.

Pencatatan

Prosedur standar pengelolaan risiko didokumentasikan dan disosialisasikan untuk kemudian digunakan dalam keseharian pengambilan keputusan. Prosedur standar diperlukan agar terjadi konsistensi mengenai langkah apa yang sebaiknya diambil dalam menghadapi situasi risiko tertentu. Hasil dari langkah tersebut didokumentasikan lebih lanjut dalam bentuk pencatatan dan pelaporan tentang hasil pengelolaan risiko sebagai bahan evaluasi dan peningkatan keefektifan prosedur standar yang ada.

Insentif

Insentif dan penghargaan diberikan kepada mereka yang dapat mengelola risiko dengan baik. Sistem insentif dan penghargaan (*reward*) sebaiknya dirancang untuk mendorong seluruh jajaran organisasi agar terbuka dalam pengelolaan risiko mereka dan terus berkomitmen serta disiplin dalam pengendalian risiko yang menjadi tanggung jawabnya. Penilaian kinerja karyawan sebaiknya juga mempertimbangkan keefektifan penerapan manajemen risiko yang sudah dilakukan sehingga dapat memotivasi mereka mengambil inisiatif untuk lebih efektif dan efisien dalam pengelolaan risiko di periode berikutnya.

Integrasi

Pengintegrasian manajemen risiko ke dalam seluruh proses bisnis organisasi dilakukan secara bertahap agar terjadi penyebaran dan penyerapan yang efektif. Pengintegrasian dapat diawali dengan mempertimbangkan dan menyelaraskan proses manajemen risiko dengan sistem manajemen kinerja organisasi, dan semakin lama semakin melebur ke dalam berbagai proses bisnis mulai dari tingkat pengambilan strategis sampai ke seluruh aspek operasional organisasi.

Evaluasi

Pengukuran indeks peningkatan budaya sadar risiko dilakukan secara rutin setidaknya satu tahun sekali. Pengukuran ini dapat menjadi alat evaluasi untuk perbaikan kualitas pengembangan budaya sadar risiko secara berkelanjutan sehingga tingkatan budaya sadar risiko dapat beranjak dan meningkat menjadi budaya peduli risiko yang lebih adaptif terhadap perkembangan organisasi. Pengukuran indeks dapat dilakukan oleh audit internal ataupun oleh penyedia jasa asurans eksternal.

CATATAN Pengukuran indeks peningkatan budaya sadar risiko dapat dilakukan sebagai inisiatif tersendiri atau menjadi bagian dari pengukuran model tingkat maturitas risiko organisasi secara keseluruhan.

Lampiran E
(informatif)
Contoh model tingkat maturitas risiko

E.1 Umum

Model tingkat maturitas risiko diperlukan sebagai rujukan organisasi untuk peningkatan dan perbaikan proses manajemen risiko pada khususnya dan implementasi manajemen risiko secara keseluruhan.

Contoh model tingkat maturitas risiko dalam lampiran ini adalah organisasi lembaga kementerian yang melibatkan pimpinan dan manajemen puncak terutama JPT Madya dalam peningkatan maturitas implementasi manajemen risiko lembaga.

Model ini juga dapat diadopsi dan/atau diadaptasi sebagai rujukan bagi organisasi sektor publik Lembaga Pemerintah Non Kementerian (LPNK). Pihak yang bertanggung jawab untuk peningkatan maturitas risiko bagi LPNK adalah pimpinan dan manajemen puncak lembaga tersebut, atau sederajat dengan Menteri dan para JPT Madya di lembaga kementerian.

CATATAN Organisasi sektor publik non lembaga kementerian perlu menyesuaikan dengan konteks masing-masing, termasuk nomenklatur yang digunakan.

E.2 Model tingkat maturitas

Di bawah ini adalah model tingkat maturitas risiko dengan lima tingkatan:

- Tingkat maturitas 1: Belum sadar risiko (*Risk naive*) dimana organisasi memiliki tingkat maturitas $\leq$ 20% dari skala 100%.
- TIngkat maturitas 2: Sudah mulai sadar risiko (*Risk aware*) dimana organisasi memiliki tingkat maturitas > 20% - $\leq$ 40% dari skala 100%.
- Tingkat maturitas 3: Sadar risiko dan risiko terdefinisi (*Risk defined)* dimana organisasi memiliki tingkat maturitas > 40% - $\leq$ 60% dari skala 100%.
- Tingkat maturitas 4: Budaya sadar risiko tercipta dan risiko terkelola (*Risk managed*) dimana organisasi memiliki tingkat maturitas > 60% - $\leq$ 80% dari skala 100%.
- Tingkat maturitas 5: Budaya sadar risiko optimal dan manajemen risiko sudah menjadi alat pemampu unggulan organisasi dalam pencapaian sasaran (*Risk enabled*), dimana organisasi memiliki tingkat maturitas > 80% - $\leq$ 100%.

Tabel E.1 – Model tingkat maturitas risiko (1 dari 2)

Tingkat maturitas	Parameter penilaian			
	Kepemimpinan	**Proses manajemen risiko**	**Aktivitas penanganan risiko**	**Hasil penerapan manajemen risiko**
Belum sadar risiko (*Risk naive*)	Kesadaran dan pemahaman pimpinan dan manajemen puncak terhadap implementasi manajemen risiko sangat rendah.	Proses manajemen risiko dilaksanakan sangat parsial, tidak terstruktur dan tidak sistematis serta sangat tidak lengkap. Identifikasi risiko sangat tidak komprehensif.	Jumlah persentase mitigasi yang dilaksanakan dan keberhasilan penurunan tingkat risiko sangat rendah.	Keberhasilan pencapaian sasaran dan tujuan strategis sangat rendah.
Sudah mulai sadar risiko (*Risk aware*)	Kesadaran dan pemahaman pimpinan dan manajemen puncak terhadap implementasi manajemen risiko rendah.	Proses manajemen risiko dilaksanakan parsial, tidak terstruktur dan tidak sistematis serta tidak lengkap. Identifikasi risiko tidak komprehensif.	Jumlah persentase mitigasi yang dilaksanakan dan keberhasilan penurunan tingkat risiko rendah.	Keberhasilan pencapaian sasaran dan tujuan strategis rendah.
Sadar risiko dan risiko terdefinisi (*Risk defined*)	Kesadaran dan pemahaman pimpinan dan manajemen puncak terhadap implementasi manajemen risiko sedang.	Proses manajemen risiko masih ada yang dilaksanakan parsial, tetapi struktur dan sistem pengelolaan risiko secara keseluruhan mulai terwujud. Identifikasi risiko cukup komprehensif.	Jumlah persentase mitigasi yang dilaksanakan dan keberhasilan penurunan tingkat risiko sedang.	Keberhasilan pencapaian sasaran dan tujuan strategis sedang.
Budaya sadar risiko tercipta dan risiko terkelola (*Risk managed*)	Kesadaran, pemahaman dan keterlibatan pimpinan dan manajemen puncak terhadap implementasi manajemen risiko tinggi.	Proses manajemen risiko dilaksanakan menyeluruh, terstruktur, sistematis dan lengkap. Identifikasi risiko komprehensif.	Jumlah persentase mitigasi yang dilaksanakan dan keberhasilan penurunan tingkat risiko tinggi.	Keberhasilan pencapaian sasaran dan tujuan strategis tinggi.

Tabel E.1 – lanjutan (2 dari 2)

Tingkat maturitas	Parameter Penilaian			
	Kepemimpinan	**Proses manajemen risiko**	**Aktivitas penanganan risiko**	**Hasil penerapan manajemen risiko**
Budaya sadar risiko optimal dan manajemen risiko sudah menjadi pemampu organisasi dalam pencapaian sasaran unggulan (*Risk enabled*)	Kesadaran, pemahaman dan keterlibatan pimpinan dan manajemen puncak terhadap implementasi manajemen risiko sangat tinggi.	Proses manajemen risiko dilaksanakan menyeluruh, terstruktur, sistematis, dan lengkap serta terintegrasi dengan semua proses bisnis organisasi. Identifikasi risiko sangat komprehensif.	Jumlah persentase migitasi yang dilaksanakan dan keberhasilan penuruhan tingkat Risiko sangat tinggi.	Keberhasilan pencapaian sasaran dan tujuan strategis sangat tinggi.

CATATAN 1 Model tingkat maturitas risiko bersifat dinamis mengikuti perkembangan konteks organisasi.

CATATAN 2 Parameter penilaian dalam tabel E.1. Model tingkat maturitas risiko adalah parameter minimum dengan empat unsur yang sedikitnya harus digunakan oleh organisasi.

CATATAN 3 Penerapan tabel model tingkat maturitas risiko membutuhkan penggunaan indikator yang relevan agar parameter penilaian dapat terukur dan dapat diperbandingkan satu sama lain.

Bibliografi

[1] SNI ISO 31004 *Manajemen risiko – Panduan untuk implementasi SNI ISO 31000*

[2] SNI IEC/ISO 31010 Manajemen risiko – Teknik penilaian risiko

[3] Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik

[4] Undang-Undang Republik Indonesia Nomor 5 Tahun 2014 Tentang Aparatur Sipil Negara

[5] Peraturan Pemerintah Republik Indonesia Nomor 60 Tahun 2008 Tentang Sistem Pengendalian Intern Pemerintah

[6] Peraturan Menteri Keuangan Republik Indonesia Nomor 12/PMK.09/2019 Tentang Penerapan Manajemen Risiko di Lingkungan Kementerian Keuangan

[7] Peraturan Menteri Keuangan Republik Indonesia Nomor 32/KMK.09/2013 Tentang Kerjangka Kerja Penerapan Pengendalian Intern di Lingkungan Kementerian Keuangan

[8] Center for Risk Management Studies Indonesia (http://crmsindonesia.org/)

Informasi pendukung terkait perumusan standar

[1] Komtek Perumusan SNI

Komite Teknis 03-10 *Tata Kelola, Manajemen Risiko, dan Kepatuhan*

[2] Susunan keanggotaan Komtek Perumusan SNI

Ketua : Antonius Alijoyo
Sekretaris : Anna Melianawati
Anggota :

1. D.S Priyarsono
2. Adnan Pandu Pradja
3. Waluyo
4. Arif Budiman
5. B. Dwita Pradana
6. Nursepdal Verliandri
7. Haryono
8. Charles Reinier Vorst
9. Ridwan Hendra
10. Mohammad Mukhlis
11. Bernado A. Mochtar
12. Wening Kusharjani
13. Johan Chandra

[3] Konseptor Rancangan SNI

1. Antonius Alijoyo
2. Taracandra Yahitadewi

[4] Sekretariat pengelola Komtek Perumusan SNI

Direktorat Pengembangan Standar Infrastruktur, Penilaian Kesesuaian, Personal dan Ekonomi Kreatif
Badan Standardisasi Nasional